Summit® WM User Guide
Software Version 5.3

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: January 2009
Part number: 120481-00 Rev 02

AccessAdapt, Alpine, Altitude, BlackDiamond, EPICenter, Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ScreenPlay, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is a registered trademark of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2008-2009 Extreme Networks, Inc. All Rights Reserved.

Table of Contents

About this guide 9

Who should use this guide 9
What is in this guide 9
Formatting conventions 10
Documentation feedback 11
Safety Information 11

Chapter 1: Overview of the Controller, Access Points, and WM software solution 15

Conventional wireless LANS 15
Elements of the Controller, Access Points, and WM software solution 16
Controller, Access Points, and WM software and your network 19
Network traffic flow 20
Network security 21
WM Access Domain Services 23
Static routing and routing protocols 23
Packet filtering policy 23
Mobility and roaming 24
Network availability 24
Quality of Service (QoS) 25
System Configuration Overview 25

Chapter 2: Configuring the Summit WM Controller 27

System configuration overview 28
Performing the first time setup of the Summit WM Controller 31
Accessing the Summit WM Controller 31
Connecting the Summit WM Controller to your enterprise network 35
Applying the product license key 36
Setting up the data ports 36
Setting up Internal VLAN ID and multi-cast support for the ports 42
Setting up static routes 43
Setting up OSPF Routing 45
Filtering at the interface level 47
Built-in port-based exception filters 48
User defined port-based exception filters 49
Configuring the login authentication mode 50
Configuring the local login authentication mode and adding new users 51
Configuring the RADIUS login authentication mode 52
Configuring network time 56
Completing the system configuration 58
Ongoing Operations of the Controller, Access Points, and WM software 58

Chapter 3: Configuring the Altitude AP 59

Altitude AP overview 59

Altitude AP....60
Outdoor AP....61
Altitude 802.11n AP....62
Altitude AP default IP address and first-time configuration....66
Assigning static IP address to Altitude AP....67
Discovery and registration overview....71
Altitude AP discovery....71
Registration after discovery....72
Understanding the Altitude AP LED status....73
Configuring the Altitude APs for the first time....80
Defining properties for the discovery process....80
Connecting the Altitude AP to a power source and initiating the discovery and registration process . 82
Adding and registering an Altitude AP manually....83
Configuring Altitude AP settings....84
Modifying an Altitude AP's status....85
Modifying an Altitude AP's properties....86
Modifying Altitude AP radio properties....88
Setting up the Altitude AP using static configuration....114
Setting up 802.1X authentication for an Altitude AP....116
Setting up 802.1X authentication for Altitude APs using Multi-edit....122
Configuring the default Altitude AP settings....125
Modifying an Altitude AP's properties based on a default AP configuration....134
Modifying the Altitude AP's default setting using the Copy to Defaults feature....134
Configuring Altitude APs simultaneously....135
Performing Altitude AP software maintenance....137

Chapter 4: WM Access Domain Services 141

WM-AD overview....141
Setting up a WM-AD checklist....142
Topology of a WM-AD....143
RF assignment for a WM-AD....145
Authentication for a WM-AD....145
Authentication with SSID network assignment....145
Authentication with AAA (802.1X) network assignment....146
Filtering for a WM-AD....146
Final filter rule....147
Filtering sequence....147
Data protection on a WM-AD - WEP and WPA....148
WM-AD global settings....149
Defining RADIUS servers for Global Settings....149
Defining Admission Control Thresholds for Global Settings....150
Defining inter-Summit WM Wireless Controller shared secret for Global Settings....151
Creating Bandwidth Control profiles....152
Setting up a new WM-AD....153

Chapter 5: WM Access Domain Services configuration.... 155

WM-AD Types....156
Creating a new WM-AD name....156

Topology for a WM-AD 156
Configuring topology for a WM-AD for Captive Portal 157
Configuring topology for a WM-AD for AAA 163
Saving your topology properties 164
Assigning Altitude AP radios to a WM-AD 164
Deleting a WM-AD 166
Authentication for a WM-AD 166
Vendor Specific Attributes 166
Defining authentication for a WM-AD for Captive Portal 167
Defining authentication for a WM-AD for AAA 174
Defining MAC-based authentication for a WM-AD 177
Defining accounting methods for a WM-AD 179
Defining RADIUS filter policy for WM-ADs and WM-AD groups 180
Configuring filtering rules for a WM-AD 181
Filtering rules for an exception filter 182
Defining non-authenticated filters 183
Filtering rules for a filter ID group 187
Filtering rules for a default filter 189
Enabling multicast for a WM-AD 191
Configuring privacy for a WM-AD 193
Privacy for a WM-AD for Captive Portal 193
Privacy for a WM-AD for AAA 196
Defining a WM-AD with no authentication 202
Defining priority level and service class for WM-AD traffic 203
Defining the service class for the WM-AD 203
Configuring the priority override 204
Working with Quality of Service (QoS) 204
QoS modes 204
Configuring the QoS policy on a WM-AD 206
Bridging traffic locally 210
Wireless Distribution System 212
Simple WDS configuration 212
Wireless Repeater configuration 213
Wireless Bridge configuration 213
Examples of deployment 214
WDS WM-AD 214
Key features of WDS 217
Deploying the WDS system 220
Changing the pre-shared key in WDS WM-AD 229

Chapter 6: Availability and session availability 231

Availability 231
Events and actions in availability 232
Availability prerequisites 233
Session availability 237
Events and actions in session availability 240
Configuring session availability 241
Viewing the Altitude AP availability display 251
Viewing SLP activity 251

Chapter 7: Mobility 253

Mobility overview 253
Mobility domain topologies 254
Configuring mobility domain 256
Displays for the mobility manager 258

Chapter 8: Working with third-party APs 259

Setting up third-party APs 259
Step 1 - Define a data port as a third party AP port 259
Step 2 - Define a WM-AD for the third-party AP port 260
Step 3 - Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD 261
Step 4 - Define filtering rules for the third-party APs 261

Chapter 9: Working with the Summit WM series Spy 263

Summit WM series Spy overview 263
Enabling the Analysis and data collector engines 264
Running Summit WM series Spy scans 265
Analysis engine overview 267
Working with Summit WM series Spy scan results 268
Working with friendly APs 270
Maintaining the Summit WM series Spy list of APs 271
Viewing the Scanner Status report 272

Chapter 10: Working with reports and displays 273

Viewing the displays 273
Viewing the Wireless AP availability display 275
Viewing statistics for Wireless APs 277
Viewing the System Information and Manufacturing Information displays 281
Viewing displays for the mobility manager 283
Viewing reports 285
Call Detail Records (CDRs) 288
CDR files 288
CDR file types 288
CDR file format 289
Viewing CDRs 291

Chapter 11: Performing system administration 297

Performing Altitude AP client management 297
Disassociating a client 297
Blacklisting a client 298
Defining management users 301
Configuring the network time 303
Configuring the network time using the system's time 303
Configuring the network time using the NTP 304
Configuring Web session timeouts 305

Glossary 307

Networking terms and abbreviations 307

Controller, Access Points, and WM software terms and abbreviations....324

Appendix A: Summit WM Controller's physical description 327

Summit WM1000 Controller front panel....327
Summit WM1000 Controller back panel....327
Summit WM100 Controller front panel....329
Summit WM100 Controller back panel....329
Summit WM200/2000 Controller front panel....330
LED states and Seven Segment Display (SSD) codes....331
Summit WM200/2000 Controller back panel....333
Summit WM20 Controller....334
Summit WM20 Controller front panel....334
Summit WM20 Controller back panel....336

Appendix B: Regulatory information.... 337

Summit WM Controller WM100/WM1000/WM20/WM200/2000....338
Conformance standards and directives....338
Altitude 350-2 and Altitude 450/451....339
Country List for Altitude 450/451 Power Adapter....339
Wi-Fi certification....340
Altitude 350-2d external antenna AP....341
Altitude 451 external antenna AP....341
United States....341
Canada....349
European community....356
Certifications of other countries....365

Appendix C: SpectraLink Wireless Telephones.... 367

Network Topology....368
Configuring Summit WM Controller for SpectraLink Telephones....369
Setting up SSID....369
Configuring filters....371
Setting up Multicast configuration....372
Setting up Security....373
Setting up Quality of Service (QoS)....374
Setting up Radio Properties....375

Index.... 377

About this guide

This guide describes how to install, configure, and manage the Extreme Networks® Summit® WM Controller, Access Points, and WM software.

This guide is based on the following product families:

- Summit WM2000 Controller
- Summit WM200 Controller
- Summit WM20 Controller
- Summit WM1000 Controller
- Summit WM100 Controller

Who should use this guide

This guide is a reference for system administrators who install and manage the Summit Controller, Access Points, and WM software system.

Any administrator performing tasks described in this guide must have an account with administrative privileges.

What is in this guide

This guide contains the following:

- "About this guide" describes the target audience and content of the guide, the formatting conventions used in it, and how to provide feedback on the guide.
- Chapter 1, "Overview of the Controller, Access Points, and WM software solution," provides an overview of the product, its features and functionality.
- Chapter 2, "Configuring the Summit WM Controller," describes how to perform the installation, first time setup and configuration of the Summit WM Controller, as well as configuring the data ports and defining routing.
- Chapter 3, "Configuring the Altitude AP," describes how to install the Wireless AP, how it discovers and registers with the Summit WM Controller, how to view and modify the radio configuration, and how to enable Dynamic Radio Management.
- Chapter 4, "WM Access Domain Services," provides an overview of WM Access Domain Services (WM-AD), the mechanism by which the Summit WM Controller, Access Points, and WM software controls and manages network access.
- Chapter 5, "WM Access Domain Services configuration," provides detailed instructions in how to configure a WM-AD, its topology, authentication, accounting, RADIUS policy, multicast, filtering and privacy. Both Captive Portal and AAA types of WM-AD are described.
- Chapter 6, "Availability and session availability" describes how to set up the features that provide availability in the event of a controller failover.

- Chapter 7, "Mobility" describes how to set up the mobility domain that provides mobility for a wireless device user when the user roams from one Altitude AP to another in the mobility domain.
- Chapter 8, "Working with third-party APs," describes how to use the Controller, Access Points, and WM software features with third-party wireless access points.
- Chapter 9, "Working with the Summit WM series Spy," describes the security tool that scans for, detects, and reports on rogue APs.
- Chapter 10, "Working with reports and displays," describes the various reports and displays available in the Summit WM Controller, Access Points, and WM software system.
- Chapter 11, "Performing system administration," describes system administration activities, such as performing Altitude AP client management, defining management users, configuring the network time, and configuring Web session timeouts.
- "Glossary" contains a list of terms and definitions for the Summit WM Controller and the Wireless AP as well as standard industry terms used in this guide.
- Appendix A, "Summit WM Controller's physical description," describes the physical description and LED states of the Summit WM Controller.
- Appendix B, "Regulatory information," provides the regulatory information for the Summit WM100/WM1000/WM20/WM200/WM2000 Wireless LAN Controllers and the Altitude™ Access Points (APs).
- Appendix C, "SpectraLink Wireless Telephones," describes how to configure NetLink Wireless Telephones and WLAN infrastructure products.

Formatting conventions

The Summit WM Controller, Access Points, and WM software documentation uses the following formatting conventions to make it easier to find information and follow procedures:

- **Bold** text is used to identify components of the management interface, such as menu items and section of pages, as well as the names of buttons and text boxes.

  For example: Click **Logout**.

- `Monospace` font is used in code examples and to indicate text that you type.

  For example: Type `https://<wm-address>[:mgmt-port>]`

- The following notes are used to draw your attention to additional information:

NOTE

Notes identify useful information, such as reminders, tips, or other ways to perform a task.

CAUTION

Cautionary notes identify essential information, which if ignored can adversely affect the operation of your equipment or software.

WARNING!

Warning notes identify essential information, which if ignored can lead to personal injury or harm.

Documentation feedback

If you have any problems using this document, please contact your next level of support:

- Extreme Networks employees should contact the interactive Customer Engagement Team (i-CET).
- Customers should contact the Extreme Networks Customer Support Center.

When you call, please have the following information ready. This will help us to identify the document that you are referring to.

- Title: Summit WM User Guide, Software Version 5.3
- Part Number: 120481-00 Rev 02

Safety Information

Dangers

- Replace the power cable immediately if it shows any sign of damage.
- Replace any damaged safety equipment (covers, labels and protective cables) immediately.
- Use only original accessories or components approved for the system. Failure to observe these instructions may damage the equipment or even violate safety and EMC regulations.
- Only authorized Extreme Networks service personnel are permitted to service the system.

Warnings

- This device must not be connected to a LAN segment with outdoor wiring.
- Ensure that all cables are run correctly to avoid strain.
- Replace the power supply adapter immediately if it shows any sign of damage.
- Disconnect all power before working near power supplies unless otherwise instructed by a maintenance procedure.
- Exercise caution when servicing hot swappable Summit WM Controller components: power supplies or fans. Rotating fans can cause serious personal injury.
- This unit may have more than one power supply cord. To avoid electrical shock, disconnect all power supply cords before servicing. In the case of unit failure of one of the power supply modules, the module can be replaced without interruption of power to the Summit WM Controller. However, this procedure must be carried out with caution. Wear gloves to avoid contact with the module, which will be extremely hot.
- There is a risk of explosion if a lithium battery is not correctly replaced. The lithium battery must be replaced only by an identical battery or one recommended by the manufacturer.
- Always dispose of lithium batteries properly.
- Do not attempt to lift objects that you think are too heavy for you.

Cautions

- Check the nominal voltage set for the equipment (operating instructions and type plate). High voltages capable of causing shock are used in this equipment. Exercise caution when measuring high voltages and when servicing cards, panels, and boards while the system is powered on.
- Only use tools and equipment that are in perfect condition. Do not use equipment with visible damage.
- To protect electrostatic sensitive devices (ESD), wear a wristband before carrying out any work on hardware.
- Lay cables so as to prevent any risk of them being damaged or causing accidents, such as tripping.

Sicherheitshinweise

Gefahrenhinweise

- Sollte das Netzkabel Anzeichen von Beschädigungen aufweisen, tauschen Sie es sofort aus.
- Tauschen Sie beschädigte Sicherheitsausrüstungen (Abdeckungen, Typenschilder und Schutzkabel) sofort aus.
- Verwenden Sie ausschließlich Originalzubehör oder systemspezifisch zugelassene Komponenten. Die Nichtbeachtung dieser Hinweise kann zur Beschädigung der Ausrüstung oder zur Verletzung von Sicherheits- und EMV-Vorschriften führen.
- Das System darf nur von autorisiertem Extreme Networks-Servicepersonal gewartet werden.

Warnhinweise

- Dieses Gerät darf nicht über Außenverdrahtung an ein LAN-Segment angeschlossen werden.
- Stellen Sie sicher, dass alle Kabel korrekt geführt werden, um Zugbelastung zu vermeiden.
- Sollte das Netzteil Anzeichen von Beschädigung aufweisen, tauschen Sie es sofort aus.
- Trennen Sie alle Stromverbindungen, bevor Sie Arbeiten im Bereich der Stromversorgung vornehmen, sofern dies nicht für eine Wartungsprozedur anders verlangt wird.
- Gehen Sie vorsichtig vor, wenn Sie an Hotswap-fähigen Summit WM Controller-Komponenten (Stromversorgungen oder Lüftern) Servicearbeiten durchführen. Rotierende Lüfter können ernsthafte Verletzungen verursachen.
- Dieses Gerät ist möglicherweise über mehr als ein Netzkabel angeschlossen. Um die Gefahr eines elektrischen Schlages zu vermeiden, sollten Sie vor Durchführung von Servicearbeiten alle Netzkabel trennen. Falls eines der Stromversorgungsmodule ausfällt, kann es ausgetauscht werden, ohne die Stromversorgung zum Summit WM Controller zu unterbrechen. Bei dieser Prozedur ist jedoch mit Vorsicht vorzugehen. Das Modul kann extrem heiß sein. Tragen Sie Handschuhe, um Verbrennungen zu vermeiden.
- Bei unsachgemäßem Austausch der Lithium-Batterie besteht Explosionsgefahr. Die Lithium-Batterie darf nur durch identische oder vom Händler empfohlene Typen ersetzt werden.
- Achten Sie bei Lithium-Batterien auf die ordnungsgemäße Entsorgung.
- Versuchen Sie niemals, ohne Hilfe schwere Gegenstände zu heben.

Vorsichtshinweise

- Überprüfen Sie die für die Ausrüstung festgelegte Nennspannung (Bedienungsanleitung und Typenschild). Diese Ausrüstung arbeitet mit Hochspannung, die mit der Gefahr eines elektrischen Schlages verbunden ist. Gehen Sie mit großer Vorsicht vor, wenn Sie bei eingeschaltetem System Hochspannungen messen oder Karten, Schalttafeln und Baugruppen warten.
- Verwenden Sie nur Werkzeuge und Ausrüstung in einwandfreiem Zustand. Verwenden Sie keine Ausrüstung mit sichtbaren Beschädigungen.
- Tragen Sie bei Arbeiten an Hardwarekomponenten ein Armband, um elektrostatisch gefährdete Bauelemente (EGB) vor Beschädigungen zu schützen.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.

Consignes de sécurité

Dangers

- Si le cordon de raccordement au secteur est endommagé, remplacez-le immédiatement.
- Remplacez sans délai les équipements de sécurité endommagés (caches, étiquettes et conducteurs de protection).
- Utilisez uniquement les accessoires d'origine ou les modules agréés spécifiques au système. Dans le cas contraire, vous risquez d'endommager l'installation ou d'enfreindre les consignes en matière de sécurité et de compatibilité électromagnétique.
- Seul le personnel de service Extreme Networks est autorisé à maintenir/réparer le système.

Avertissements

- Cet appareil ne doit pas être connecté à un segment de LAN à l'aide d'un câblage extérieur.
- Vérifiez que tous les câbles fonctionnent correctement pour éviter une contrainte excessive.
- Si l'adaptateur d'alimentation présente des dommages, remplacez-le immédiatement.
- Coupez toujours l'alimentation avant de travailler sur les alimentations électriques, sauf si la procédure de maintenance mentionne le contraire.
- Prenez toutes les précautions nécessaires lors de l'entretien/réparations des modules du Summit WM Controller pouvant être branchés à chaud : alimentations électriques ou ventilateurs.Les ventilateurs rotatifs peuvent provoquer des blessures graves.
- Cette unité peut avoir plusieurs cordons d'alimentation.Pour éviter tout choc électrique, débranchez tous les cordons d'alimentation avant de procéder à la maintenance.En cas de panne d'un des modules d'alimentation, le module défectueux peut être changé sans éteindre le Summit WM Controller. Toutefois, ce remplacement doit être effectué avec précautions. Portez des gants pour éviter de toucher le module qui peut être très chaud.
- Le remplacement non conforme de la batterie au lithium peut provoquer une explosion. Remplacez la batterie au lithium par un modèle identique ou par un modèle recommandé par le revendeur.
- Sa mise au rebut doit être conforme aux prescriptions en vigueur.
- N'essayez jamais de soulever des objets qui risquent d'être trop lourds pour vous.

Précautions

- Contrôlez la tension nominale paramétrée sur l'installation (voir le mode d'emploi et la plaque signalétique). Des tensions élevées pouvant entraîner des chocs électriques sont utilisées dans cet équipement. Lorsque le système est sous tension, prenez toutes les précautions nécessaires lors de la mesure des hautes tensions et de l'entretien/réparation des cartes, des panneaux, des plaques.
- N'utilisez que des appareils et des outils en parfait état. Ne mettez jamais en service des appareils présentant des dommages visibles.
- Pour protéger les dispositifs sensibles à l'électricité statique, portez un bracelet antistatique lors du travail sur le matériel.
- Acheminez les câbles de manière à ce qu'ils ne puissent pas être endommagés et qu'ils ne constituent pas une source de danger (par exemple, en provoquant la chute de personnes).

1 Overview of the Controller, Access Points, and WM software solution

This chapter describes Summit WM Controller, Access Points, and WM software concepts, including:

- "Conventional wireless LANS" on page 15
- "Elements of the Controller, Access Points, and WM software solution" on page 16
- "Controller, Access Points, and WM software and your network" on page 19
- "System Configuration Overview" on page 25

The next generation of Extreme Networks wireless networking devices provides a truly scalable WLAN solution. Extreme Networks Wireless APs are fit access points controlled through a sophisticated network device, the Summit WM Controller. This solution provides the security and manageability required by enterprises and service providers.

The Controller, Access Points, and WM software system is a highly scalable Wireless Local Area Network (WLAN) solution developed by Extreme Networks. Based on a third generation WLAN topology, the Controller, Access Points, and WM software system makes wireless practical for service providers as well as medium and large-scale enterprises.

The Controller, Access Points, and WM software system provides a secure, highly scalable, cost-effective solution based on the IEEE 802.11 standard. The system is intended for enterprise networks operating on multiple floors in more than one building, and is ideal for public environments, such as airports and convention centers that require multiple access points.

This chapter provides an overview of the fundamental principles of the Controller, Access Points, and WM software system.

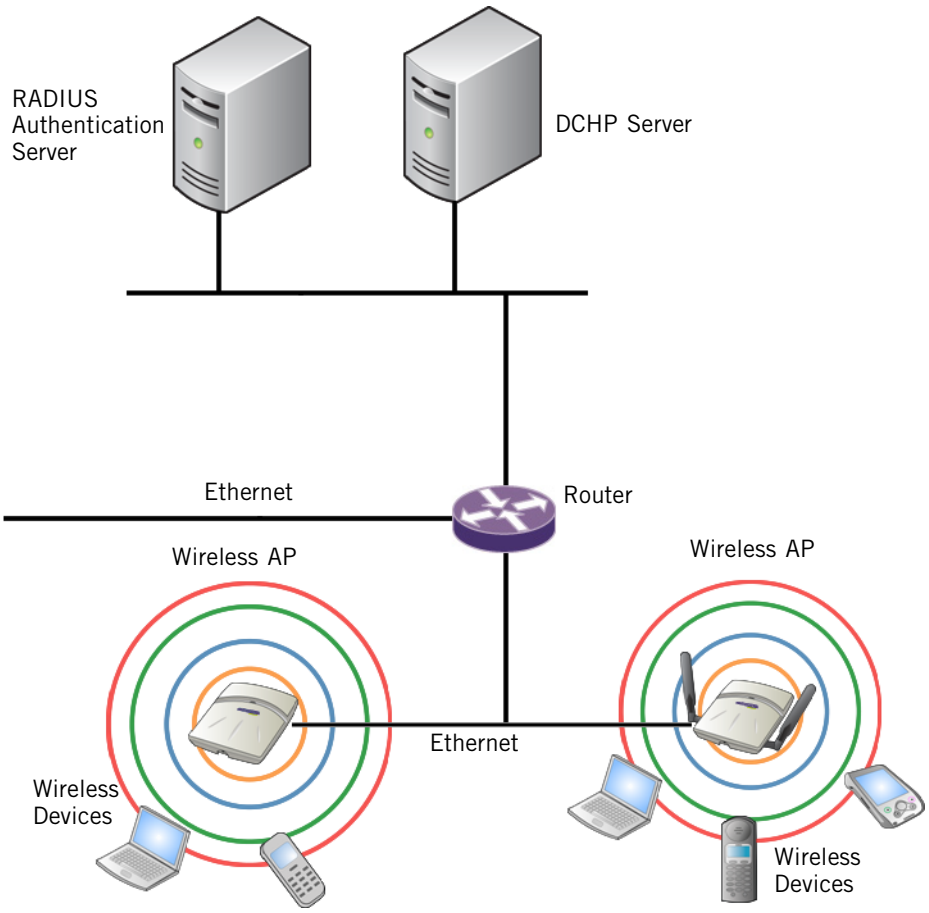
Conventional wireless LANS

Wireless communication between multiple computers requires that each computer is equipped with a receiver/transmitter - a WLAN Network Interface Card (NIC) - capable of exchanging digital information over a common radio frequency. This is called an ad hoc network configuration. An ad hoc network configuration allows wireless devices to communicate together. This setup is defined as an independent basic service set (IBSS).

An alternative to the ad hoc configuration is the use of an access point. This may be a dedicated hardware bridge or a computer running special software. Computers and other wireless devices communicate with each other through this access point. The 802.11 standard defines access point communications as devices that allow wireless devices to communicate with a distribution system. This setup is defined as a basic service set (BSS) or infrastructure network.

To allow the wireless devices to communicate with computers on a wired network, the access points must be connected to the wired network providing access to the networked computers. This topology is called bridging. With bridging, security and management scalability is often a concern.

Figure 1: Standard wireless network solution example



The wireless devices and the wired networks communicate with each other using standard networking protocols and addressing schemes. Most commonly, Internet Protocol (IP) addressing is used.

Elements of the Controller, Access Points, and WM software solution

The Controller, Access Points, and WM software solution consists of two devices:

- Summit WM Controller
- Wireless APs

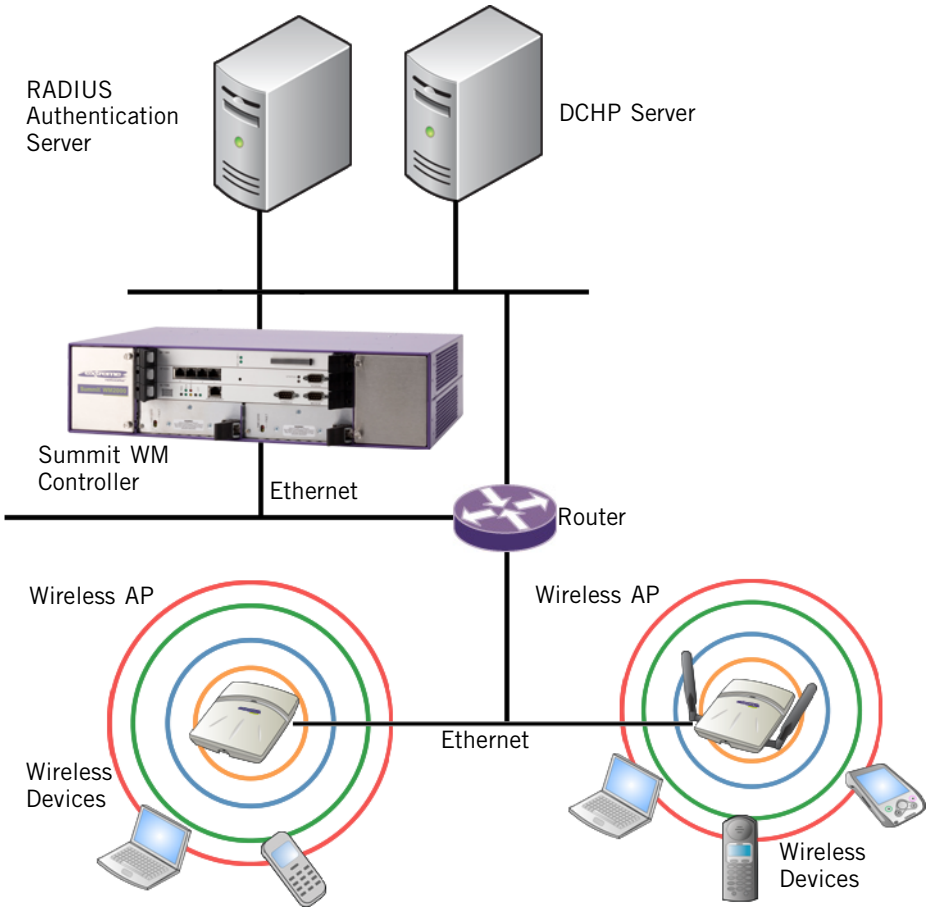
This architecture allows a single Summit WM Controller to control many Wireless APs, making the administration and management of large networks much easier.

There can be several Summit WM Controllers in the network, each with a set of registered Wireless APs. The Summit WM Controllers can also act as backups to each other, providing stable network availability.

In addition to the Summit WM Controllers and Wireless APs, the solution requires three other components, all of which are standard for enterprise and service provider networks:

- **RADIUS Server** (Remote Access Dial-In User Service) or other authentication server
- **DHCP Server** (Dynamic Host Configuration Protocol) If you do not have a DHCP Server on your network, you can enable the local DHCP Server on the Summit WM Controller. The local DHCP Server is useful as a general purpose DHCP Server for small subnets. For more information, see "Setting up the data ports" on page 36.
- **SLP** (Service Location Protocol)

Figure 2: Extreme Networks Summit WM Controller solution



As illustrated in Figure 2, the Summit WM Controller appears to the existing network as if it were an access point, but in fact one Summit WM Controller controls many Wireless APs. The Summit WM Controller has built-in capabilities to recognize and manage the Wireless APs. The Summit WM Controller:

- Activates the Wireless APs
- Enables Wireless APs to receive wireless traffic from wireless devices
- Processes the data traffic from the Wireless APs
- Forwards or routes the processed data traffic out to the network
- Authenticates requests and applies access policies

Simplifying the Wireless APs makes them cost-effective, easy to manage, and easy to deploy. Putting control on an intelligent centralized Summit WM Controller enables:

- Centralized configuration, management, reporting, and maintenance
- High security
- Flexibility to suit enterprise
- Scalable and resilient deployments with a few Summit WM Controllers controlling hundreds of Wireless APs

The Summit WM Controller, Access Points, and WM software system:

- **Scales up to Enterprise capacity** - One Summit WM100/1000 controller controls as many as 200 Wireless APs. One Summit WM20 controller controls as many as 32 Wireless APs and one Summit WM200/2000 controller controls as many as 200 Wireless APs. In turn each Wireless AP can handle up to 254 wireless devices, with each radio supporting a maximum of 128. With additional Summit WM Controllers, the number of wireless devices the solution can support can reach into the thousands.
- **Integrates with existing network** - A Summit WM Controller can be added to an existing enterprise network as a new network device, greatly enhancing its capability without interfering with existing functionality. Integration of the Summit WM Controllers and Wireless APs does not require any reconfiguration of the existing infrastructure (for example, VLANs).
- **Offers centralized management and control** - An administrator accesses the Summit WM Controller in its centralized location to monitor and administer the entire wireless network. From the Summit WM Controller the administrator can recognize, configure, and manage the Wireless APs and distribute new software releases.
- **Provides easy deployment of Wireless APs** - The initial configuration of the Wireless APs on the centralized Summit WM Controller can be done with an automatic "discovery" technique. For more information, see "Discovery and registration overview" on page 71.
- **Provides security via user authentication** - Uses existing authentication (AAA) servers to authenticate and authorize users.
- **Provides security via filters and privileges** - Uses virtual networking techniques to create separate Access Domains with defined authentication and billing services, access policies, and privileges.
- **Supports seamless mobility and roaming** - Supports seamless roaming of a wireless device from one Wireless AP to another on the same Summit WM Controller or on a different Summit WM Controller.
- **Integrates third-party access points** - Uses a combination of network routing and authentication techniques.
- **Prevents rogue devices** - Unauthorized access points are detected and identified as harmless or dangerous rogue APs.
- **Provides accounting services** - Logs wireless user sessions, user group activity, and other activity reporting, enabling the generation of consolidated billing records.
- **Offers troubleshooting capability** - Logs system and session activity and provides reports to aid in troubleshooting analysis.
- **Offers Dynamic Radio Management** - Automatically selects channels and adjusts Radio Frequency (RF) signal propagation and power levels without user intervention.

Controller, Access Points, and WM software and your network

This section is a summary of the components of the Controller, Access Points, and WM software solution on your enterprise network. The following are described in detail in this guide, unless otherwise stated:

- **Summit WM Controller** - A rack-mountable network device that provides centralized control over all access points (both Wireless APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
- **Wireless AP** - A wireless LAN fit access point (IEEE 802.11) that communicates only with a Summit WM Controller.
- **RADIUS Server** (Remote Access Dial-In User Service) (RFC2865), or other authentication server - An authentication server that assigns and manages ID and Password protection throughout the network. Used for authentication of the wireless users in either 802.1X or Captive Portal security modes. The RADIUS Server system can be set up for certain standard attributes, such as filter ID, and for the Vendor Specific Attributes (VSAs). In addition, Radius Disconnect (RFC3576) which permits dynamic adjustment of user policy (user disconnect) is supported.
- **DHCP Server** (Dynamic Host Configuration Protocol) (RFC2131) - A server that assigns IP addresses, gateways, and subnet masks dynamically. IP address assignment for clients can be done by the DHCP server internal to the Summit WM Controller, or by existing servers using DHCP relay. It is also used by the Wireless APs to discover the location of the Summit WM Controller during the initial registration process. For SLP, DHCP should have Option 78 enabled. Option 78 specifies the location of one or more SLP Directory Agents.
- **Service Location Protocol (SLP)** (SLP RFC2608) - Client applications are User Agents and services that are advertised by a Service Agent. In larger installations, a Directory Agent collects information from Service Agents and creates a central repository. The Extreme Networks solution relies on registering "extreme" as an SLP Service Agent.

NOTE

The WM is discovered by identifying it as an SLP Directory Agent.

- **Domain Name Server (DNS)** - A server used as an alternate mechanism (if present on the enterprise network) for the automatic discovery process. Controller, Access Points, and WM software relies on the DNS for Layer 3 deployments and for static configuration of Wireless APs. The controller can be registered in DNS, to provide DNS assisted AP discovery.
- **Web Authentication Server** - A server that can be used for external Captive Portal and external authentication. The Summit WM Controller has an internal Captive portal presentation page, which allows Web authentication (Web redirection) to take place without the need for an external Captive Portal server.
- **RADIUS Accounting Server** (Remote Access Dial-In User Service) (RFC2866) - A server that is required if RADIUS Accounting is enabled.
- **Simple Network Management Protocol** (SNMP) - A Manager Server that is required if forwarding SNMP messages is enabled.
- **Check Point Server** (Check Point Event Logging API) - A server for security event logging that is required if a firewall application is enabled. Checkpoint ELA certification for OPSEC is provided.
- **Network infrastructure** - The Ethernet switches and routers must be configured to allow routing between the various services noted above. Routing must also be enabled between multiple Summit WM Controllers for the following features to operate successfully:

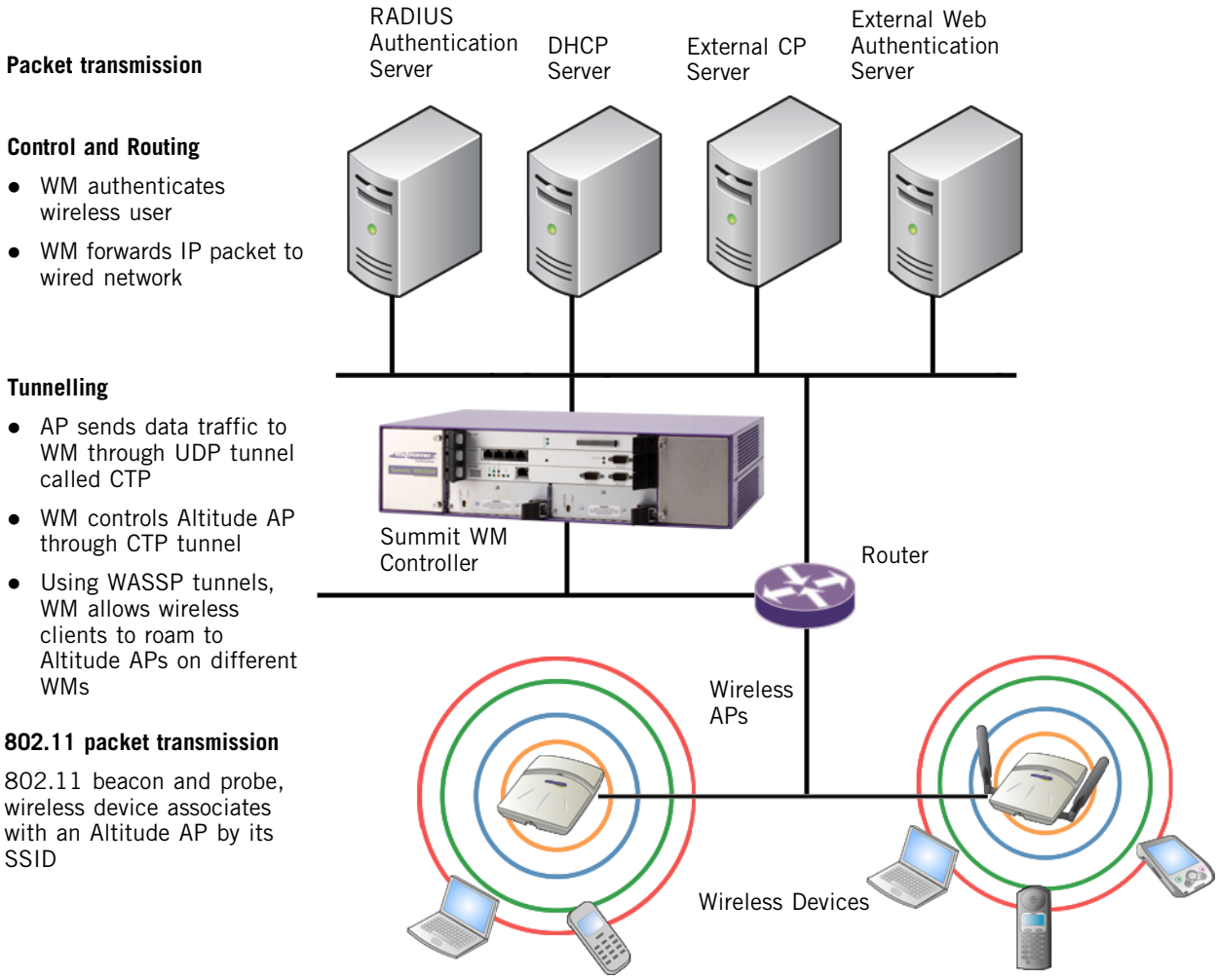
  - Availability
  - Mobility
  - Summit WM series Spy for detection of rogue access points

  Some features also require the definition of static routes.
- **Web Browser** - A browser provides access to the Summit WM Controller Management user interface to configure the Controller, Access Points, and WM software.
- **SSH Enabled Device** - A device that supports Secure Shell (SSH) is used for remote (IP) shell access to the system.
- **Zone Integrity** - The Zone integrity server enhances network security by ensuring clients accessing your network are compliant with your security policies before gaining access. Zone Integrity Release 5 is supported.

Network traffic flow

Figure 3 illustrates a simple configuration with a single Summit WM Controller and two Wireless APs, each supporting a wireless device. A RADIUS server on the network provides authentication, and a DHCP server is used by the Wireless APs to discover the location of the Summit WM Controller during the initial registration process. Network inter-connectivity is provided by the infrastructure routing and switching devices.

Figure 3: Traffic Flow diagram


Packet transmission
Control and Routing
• WM authenticates wireless user
• WM forwards IP packet to wired network
Tunnelling
• AP sends data traffic to WM through UDP tunnel called CTP
• WM controls Altitude AP through CTP tunnel
• Using WASSP tunnels, WM allows wireless clients to roam to Altitude APs on different WMs
802.11 packet transmission
802.11 beacon and probe, wireless device associates with an Altitude AP by its SSID
RADIUS Authentication Server
DHCP Server
External CP Server
External Web Authentication Server
Summit WM Controller
Router
Wireless APs
Wireless Devices

Each wireless device sends IP packets in the 802.11 standard to the Wireless AP. The Wireless AP uses a UDP (User Datagram Protocol) based tunnelling protocol to encapsulate the packets and forward them to the Summit WM Controller. The Summit WM Controller decapsulates the packets and routes these to destinations on the network.

The Summit WM Controller functions like a standard router, except that it is configured to route only network traffic associated with wireless connected users. The Summit WM Controller can also be configured to simply forward traffic to a default or static route if dynamic routing is not preferred.

Network security

The Controller, Access Points, and WM software system provides features and functionality to control network access. These are based on standard wireless network security practices.

Current wireless network security methods provide protection. These methods include:

- Shared Key authentication that relies on Wired Equivalent Privacy (WEP) keys
- Open System that relies on Service Set Identifiers (SSIDs)

- 802.1X that is compliant with Wi-Fi Protected Access (WPA)
- Captive Portal based on Secure Sockets Layer (SSL) protocol

The Controller, Access Points, and WM software system provides the centralized mechanism by which the corresponding security parameters are configured for a group of APs.

- Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the 802.11b standard
- Wi-Fi Protected Access version 1 WPA1(TM) with Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access version 2 WPA2(TM) with Advanced Encryption Standard (AES) and Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP)

Authentication

The Summit WM Controller relies on a RADIUS server, or authentication server, on the enterprise network to provide the authentication information (whether the user is to be allowed or denied access to the network). A RADIUS client is implemented to interact with infrastructure RADIUS servers.

The Summit WM Controller provides authentication using:

- Captive Portal - a browser-based mechanism that forces users to a Web page
- RADIUS (using IEEE 802.1X)

The 802.1X mechanism is a standard for authentication developed within the 802.11 standard. This mechanism is implemented at the wireless Port, blocking all data traffic between the wireless device and the network until authentication is complete. Authentication by 802.1X standard uses Extensible Authentication Protocol (EAP) for the message exchange between the Summit WM Controller and the RADIUS server.

When 802.1X is used for authentication, the Summit WM Controller provides the capability to dynamically assign per-wireless-device WEP keys (called per-session WEP keys in 802.11). Or in the case of WPA, the Summit WM Controller is not involved in key assignment. Instead, the controller is involved in the path between RADIUS server and the user to negotiate the appropriate set of keys. With WPA2 the material exchange produces a Pairwise Master Key which is used by the AP and the user to derive their temporal keys. (The keys change over time.)

In the Controller, Access Points, and WM software, a RADIUS redundancy feature is provided, where you can define a failover RADIUS server (up to 2 servers) in the event that the active RADIUS server fails.

Privacy

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques.

Controller, Access Points, and WM software supports the Wired Equivalent Privacy (WEP) standard common to conventional access points.

It also provides Wi-Fi Protected Access version 1 (WPA v.1) encryption, based on Pairwise Master Key (PMK) and Temporal Key Integrity Protocol (TKIP). The most secure encryption mechanism is WPA version 2, using Advanced Encryption Standard (AES).

WM Access Domain Services

WM Access Domain Services (WM-AD) provide a versatile method of mapping wireless networks to the topology of an existing wired network.

When you set up WM-AD on the Summit WM Controller you are defining subnets for groups of wireless users. The WM-AD definition provides the binding between WM-AD IP topology configuration (Routing, DHCP policy) and the RF configuration parameters that advertise and control network access (SSID, Privacy policy: WEP and WPA). This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information on user sessions that can be used for billing.

When a WM-AD is set up on the Summit WM Controller:

- One or more Wireless APs (by radio) are associated with it
- A range of IP addresses is set aside for the Summit WM Controller's DHCP server to assign to wireless devices

The Summit WM Controller can support the following:

- WM200/2000 - Up to 64 WM-ADs
- WM20 - Up to 8 WM-ADs
- WM1000 - Up to 50 WM-ADs
- WM100 - Up to 32 WM-ADs

The Wireless AP radios can be assigned to each of the configured WM-ADs in a system. Each Altitude™ AP can be the subject of 16 WM-AD assignments - 8 WM-AD assignments per radio - which corresponds to the number of SSIDs it can support. Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

Static routing and routing protocols

Routing can be used on the Summit WM Controller to support the WM-AD definitions. Through the user interface you can configure routing on the Summit WM Controller to use one of the following routing techniques:

- **Static routes** - Use static routes to set the default route of a Summit WM Controller so that legitimate wireless device traffic can be forwarded to the default gateway.
- **Open Shortest Path First** (OSPF, version 2) (RFC2328) - Use OSPF to allow the Summit WM Controller to participate in dynamic route selection. OSPF is a protocol designed for medium and large IP networks with the ability to segment routes into different areas by routing information summarization and propagation. Static Route definition and OSPF dynamic learning can be combined, but a static route definition will take precedence over dynamic rules.
- **Next-hop routing** - Use next-hop routing to specify a unique gateway to which traffic on a WM-AD is forwarded. Defining a next-hop for a WM-AD forces all the traffic in the WM-AD to be forwarded to the indicated network device, bypassing any routing definitions of the controller's route table.

Packet filtering policy

Policy refers to the rules that allow different groups of users access to the network. The Controller, Access Points, and WM software system can link authorized users to user groups. These user groups then can be confined to predefined portions of the network.

In the Controller, Access Points, and WM software system, network access policy is carried out by means of packet filtering within a WM-AD.

In the Summit WM Controller user interface, you set up a packet filtering policy by defining a set of hierarchical rules that allow or deny traffic to specific IP addresses, IP address ranges, or service ports. The sequence and hierarchy of these filtering rules must be carefully designed based on your enterprise user access plan.

The authentication technique selected determines how filtering is carried out:

- If authentication is by SSID and Captive Portal, a non-authenticated filter allows all users to get as far as the Captive Portal Web page, where logon authentication occurs. When authentication is returned, then filters are applied, based on user ID and permissions.
- If authentication is by AAA (802.1X), users have logged on and have been authenticated before being assigned an IP address. When authentication is completed, the authenticated filter is assigned by default unless a more user-specific filter is returned or indicated by the authentication mechanism. The characteristics and level of access for a filter are controlled and defined by the system administrator.

Mobility and roaming

In typical configurations that are not Summit WM, APs are setup as bridges that bridge wireless traffic to the local subnet. In bridging configurations, the user obtains an IP address from the same subnet as the AP. If the user roams within APs on the same subnet, it is able to keep using the same IP address. However, if the user roams to another AP outside of that subnet, its IP address is no longer valid. The user's client device must recognize that the IP address it has is no longer valid and re-negotiate a new one on the new subnet. The protocol does not mandate any action on the user. The recovery procedure is entirely client dependent. Some clients automatically attempt to obtain a new address on roam (which affects roaming latency), while others will hold on to their IP address. This loss of IP address continuity seriously affects the client's experience in the network, because in some cases it can take minutes for a new address to be negotiated.

The Controller, Access Points, and WM software solution centralizes the user's network point of presence, therefore abstracting and decoupling the user's IP address assignment from that of the APs location subnet. That means that the user is able to roam across any AP without loosing its own IP address, regardless of the subnet on which the serving APs are deployed.

In addition, a Summit WM Controller can learn about other Summit WM Controllers on the network and then exchange client session information. This enables a wireless device user to roam seamlessly between different Wireless APs on different Summit WM Controllers.

Network availability

The Controller, Access Points, and WM software provides availability against Altitude AP outages, Summit WM Controller outages, and even network outages. The Summit WM Controller (WM20/WM200/2000 platforms) in a VLAN bridged WM-AD can potentially allow the user to retain the IP address in a failover scenario, if the WM-AD/VLAN is common to both controllers. For example, availability is provided by defining a paired controller configuration by which each peer can act as the backup controller for the other's APs. APs in one controller are allowed to failover and register with the alternate controller.

If a Summit WM Controller fails, all of its associated Wireless APs can automatically switch over to another Summit WM Controller that has been defined as the secondary or backup Summit WM

Controller. If the AP reboots, the original Summit WM Controller is restored. The original Summit WM Controller is restored if it is active. However, active APs will continue to be attached to the failover controller until the administrator releases them back to the original home controller.

Quality of Service (QoS)

Controller, Access Points, and WM software provides advanced Quality of Service (QoS) management to provide better network traffic flow. Such techniques include:

- **WMM (Wi-Fi Multimedia)** - WMM is enabled per WM-AD. The Summit WM Controller provides centralized management of these AP features. For devices with WMM enabled, the standard provides multimedia enhancements for audio, video, and voice applications. WMM shortens the time between transmitting packets for higher priority traffic. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service)** or **DSCP (Diffserv Codepoint)** - The **ToS/DSCP** field in the IP header of a frame indicates the priority and QoS for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header - this is referred to as Adaptive QoS.

Quality of Service (QoS) management is also provided by:

- Assigning high priority to an SSID (configurable)
- Adaptive QoS (automatic)
- Support for legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic (configurable)

System Configuration Overview

To set up and configure the Summit WM Controller and Wireless APs, follow these steps:

1. First time Setup - Perform "First Time Setup" of the Summit WM Controller on the physical network to modify the Management Port IP address for the enterprise network.
2. Product Key - Apply a Product Key file, for licensing purposes. If no Product Key is enabled, the Summit WM Controller functions with some features enabled in demonstration mode. Not all features are enabled in this mode. For example, mobility is not enabled and cannot be used.
3. Data Port Setup - Set up the Summit WM Controller on the network by configuring the physical data ports and their function as "host port", "router port", or "3rd party AP port".
4. Routing Setup - Configure static routes and OSPF parameters for any port defined as a router port, if appropriate to the network.
5. Wireless AP Initial Setup - Connect the Wireless APs to the Summit WM Controller. They will automatically begin the Discovery of the Summit WM Controller, based on factors that include:
   - Their Registration mode (on the **Altitude AP Registration** page)
   - The enterprise network services that will support the discovery process

   The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have the same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including WM-AD assignment) upon initial registration with the Summit WM Controller.

6 Wireless AP Configuration - Modify properties or settings of the Wireless AP, if applicable.

7 WM Access Domain Services (WM-AD) Setup - Set up one or more Access Domains on the Summit WM Controller. For each WM-AD, configure the following:

- **Topology** - Configure the WM-AD.
- **RF** - Assign the Wireless APs' radios to the WM-AD.
- **Authentication and Accounting** - Configure the authentication method for the wireless device user and enable the accounting method.
- **RAD Policy** - Define filter ID values and WM-AD Groups
- **Filtering** - Define filtering rules to control network access
- **Multicast** - Define groups of IP addresses for multicast traffic
- **Privacy** - Select and configure the wireless security method on the WM-AD.
- **QoS Policy** - Configure the Qos Policy.

2 Configuring the Summit WM Controller

This chapter introduces the Summit WM Controller and describes the steps involved in its initial configuration and setup, including:

- "System configuration overview" on page 28
- "Performing the first time setup of the Summit WM Controller" on page 31
- "Configuring network time" on page 56
- "Completing the system configuration" on page 58
- "Ongoing Operations of the Controller, Access Points, and WM software" on page 58

The Summit WM Controller is a network device designed to integrate with an existing wired Local Area Network (LAN). The rack-mountable Summit WM Controller provides centralized management, network access, and routing to wireless devices that use Altitude APs to access the network. It can also be configured to handle data traffic from third-party access points.

The Summit WM Controller provides the following functionality:

- Controls and configures Altitude APs, providing centralized management
- Authenticates wireless devices that contact a Altitude AP
- Assigns each wireless device to a WM-AD when it connects
- Routes traffic from wireless devices, using WM-AD, to the wired network
- Applies filtering policies to the wireless device session
- Provides session logging and accounting capability

Summit WM Controller product family and license:

- The Summit WM Controller is available in the following product families:

Table 1: Summit WM Controller product families

Summit WM Controller Model Number	Specifications
WM100	• Four fast-Ethernet ports (10/100 BaseT), supporting up to 75 Altitude APs • One management port (10/100BaseT) • One console port (DB9 serial) • Power supply redundant (R)
WM1000	• Two GigE ports (dual 1GB SX network interfaces) supporting up to 200 Altitude APs • One management port (10/100BaseT) • One console port (DB9 serial) • Power supply standard (S)/Power supply redundant (R)

Table 1: Summit WM Controller product families (Continued)

Summit WM Controller Model Number	Specifications
WM20	• Two Data ports (10/100/1000 BaseT) • One Management port (10/100 BaseT) • One USB Control (console) port • One USB Server port (future use) • Built-in PSU, Hard Drive, Fans and Controller card - not field replaceable • Supporting up to 32 APs
WM200	• Four Data ports (10/100/1000 BaseT) • One Management port (10/100 BaseT) • One Console port (DB9 serial) • Redundant and Field Replaceable Power modules • Redundant and Field Replaceable Fan modules • Field Replaceable Supervisory module • Field Replaceable Network Processor module • Field Replaceable Flash drive module • Support up to 100 APs
WM2000	• Four Data ports (10/100/1000 BaseT) • One Management port (10/100 BaseT) • One Console port (DB9 serial) • Redundant and Field Replaceable Power modules • Redundant and Field Replaceable Fan Modules • Field Replaceable Supervisory module • Field Replaceable Network Processor module • Field Replaceable Flash drive module • Support up to 200 APs

System configuration overview

The following section provides a high-level overview of the steps involved in the initial configuration of your system:

Step 1 - Before you begin configuration

Research the type of WLAN deployment that is required.

Step 2 - Preparing the network

Ensure relevant DHCP servers and RADIUS servers (if applicable) are available and configured.

Step 3 - Installing the hardware

Install the Summit WM Controller. For more information, see the following:

- *Summit WM200/2000 Installation Guide*
- *Summit WM20 Installation Guide*
- *Summit WM100/WM1000 Installation Guide*

NOTE

The connection of a separate protective earth wire at the terminal on the rear side of the Summit WM Controller WM20 is optional.

Step 4 - Performing the first time setup

Perform the first time Setup of the Summit WM Controller on the physical network, which includes configuring the physical port IP:

- Configure the default IP address to be the relevant subnet point of attachment to the existing network. The default IP address is 10.0.#.1.
- Setup the routing protocol table.
- Configure the time zone, and then restart the Summit WM Controller. Because changing the time zone requires restarting the Summit WM Controller, it is recommended that you configure the time zone during the initial installation and configuration of the Summit WM Controller to avoid network interruptions. For more information, see "Configuring the network time" on page 303.
- To configure a physical port to attach to a VLAN, define the VLAN as part of the IP address assignment.

Applying the product license key

Apply a product license key file. If a product license key is not applied, the Summit WM Controller functions with some features enabled in demonstration mode. Not all features are enabled in demonstration mode. For example, mobility is not enabled and cannot be used.

CAUTION

Whenever the licensed region changes on the Summit WM Controller, all Altitude APs are changed to ***Auto Channel Select*** *to prevent possible infractions to local RF regulatory requirements. If this occurs, all manually configured radio channel settings will be lost.*

Installing the new license key before upgrading will prevent the Summit WM Controller from changing the licensed region, and in addition, manually configured channel settings will be maintained. For more information, see the Summit WM Maintenance Guide.

Configuring for remote access

In addition, the first time setup also involves configuring for remote access, which includes:

- Setting up an administration station (laptop) on subnet 192.168.10.0/24. By default, the controller's interface is configured with static IP 192.168.10.1.
- Configuring the system management interface.

- Configuring the data interfaces.

  Set up the Summit WM Controller on the network by configuring the physical data ports and their function as "host port", "router port", or "3rd party AP port".

- Configure the routing table.

  Configure static routes or OSPF parameters for any port defined as a router port, if appropriate to the network.

For more information, see "Performing the first time setup of the Summit WM Controller" on page 31.

Step 5 - Configuring the WM-AD

Research and then configure the traffic topologies your network must support. Set up one or more WM Access Domains on the Summit WM Controller. For each WM-AD, configure the following:

- **Topology** - Configure the WM-AD.
- **RF** - Assign the Altitude APs' radios to the WM-AD.
- **Authentication and Accounting** - Configure the authentication method for the wireless device user and enable the accounting method. The authentication and accounting configuration is optional. It only applies to Captive Portal or AAA WM-ADs.
- **RAD Policy** - Define filter ID values and WM-AD Groups. This configuration is optional.
- **Filtering** - Define filtering rules to control network access
- **Multicast** - Define groups of IP addresses for multicast traffic. This configuration is optional. By default, the multicast feature is disabled.
- **Privacy** - Select and configure the wireless security method on the WM-AD.
- **QoS Policy** - Configure the Qos Policy.

For more information, see Chapter 4, "WM Access Domain Services."

Step 6 - Registering and assigning APs to the WM-AD

Deploy Altitude APs to their corresponding network locations. Attach the Altitude APs to the network infrastructure. Once the Altitude APs are powered on, they automatically begin the Discovery process of the Summit WM Controller, based on factors that include:

- Their Registration mode (on the **Altitude AP Registration** page)
- The enterprise network services that will support the discovery process

A new feature available in the 4.0 release is a default AP configuration. The default AP configuration allows for a definition of a default configuration template, whereby APs automatically receive complete configuration. For typical deployments where all APs are to all have same configuration, this feature will expedite deployment, as an AP will automatically receive full configuration (including WM-AD assignment) upon initial registration with the Summit WM Controller. If applicable, modify the properties or settings of the Altitude APs.

For more information, see Chapter 3, "Configuring the Altitude AP."

Step 7 - Confirming the AP firmware version

Confirm the latest firmware version is loaded. For more information, see "Performing Altitude AP software maintenance" on page 137.

Performing the first time setup of the Summit WM Controller

Before you can connect the Summit WM Controller to the enterprise network, you must change the IP address of the Summit WM Controller management port from its factory default to the IP address suitable for your enterprise network. Access the Summit WM Controller by one of two methods:

- Use a device supporting VT100 emulation, attached to the DB9 serial port (COM1 port) of the Summit WM Controller via a cross-over (null modem) cable. Use the Command Line Interface (CLI) commands. For more information, see the *Summit WM CLI Reference Guide*.
- Use a laptop computer with a Web browser. Connect the supplied cross-over Ethernet cable between the laptop and management Ethernet port of the Summit WM Controller. Follow the steps below.

Accessing the Summit WM Controller

1 Statically assign an unused IP address in the 192.168.10.0/24 subnet for the Ethernet port of the computer. For example, 192.168.10.205.

2 Launch your Web browser (Internet Explorer version 6.0 or higher, or FireFox).

3 In the browser address bar, type the following:

```
https://192.168.10.1:5825
```

This launches the Summit WM GUI. The login page is displayed.

Extreme Networks Summit™ WM-Series Console
Summit™ WM-Series Home
Extreme Networks - Summit WM-Series WLAN Controller Software
Please Login to access pages of Summit WM-Series WLAN Controller Software.
If you do not have the login information, please contact your administrator.
User Name:
Password:
Login

4 In the **User Name** box, type your user name. The default is `admin`.

5 In the **Password** box, type your password. The default is `abc123`.

NOTE

To reinforce security protection, the login password length has now been increased to eight characters.

- The Summit WM Controller continues to be shipped from the factory with a six character default password (`abc123`). Although, when the Summit WM Controller is installed and you elect to change the default password, the eight character constraint will be applied.

- The new password length constraint is not applied to existing passwords. When a six character password is already being used and an upgrade of the software to V5 is performed, the software does not require the password to be changed to eight characters. However, once the upgrade is completed and a new account is created, or the password of an existing account is changed, the new password length requirement will be enforced.

- If you reset the Summit WM Controller, the login user name and the password will also reset to the factory defaults (`admin` and `abc123`).

NOTE

You can configure either the local login authentication mode, or the RADIUS login authentication mode to authenticate the user's login attempts. While the local login authentication mode uses locally configured login

and passwords, the RADIUS login authentication mode uses the RADIUS Server to authenticate the users' login attempts.

NOTE

The local login authentication mode is enabled by default. For more information see "Configuring the login authentication mode" on page 50

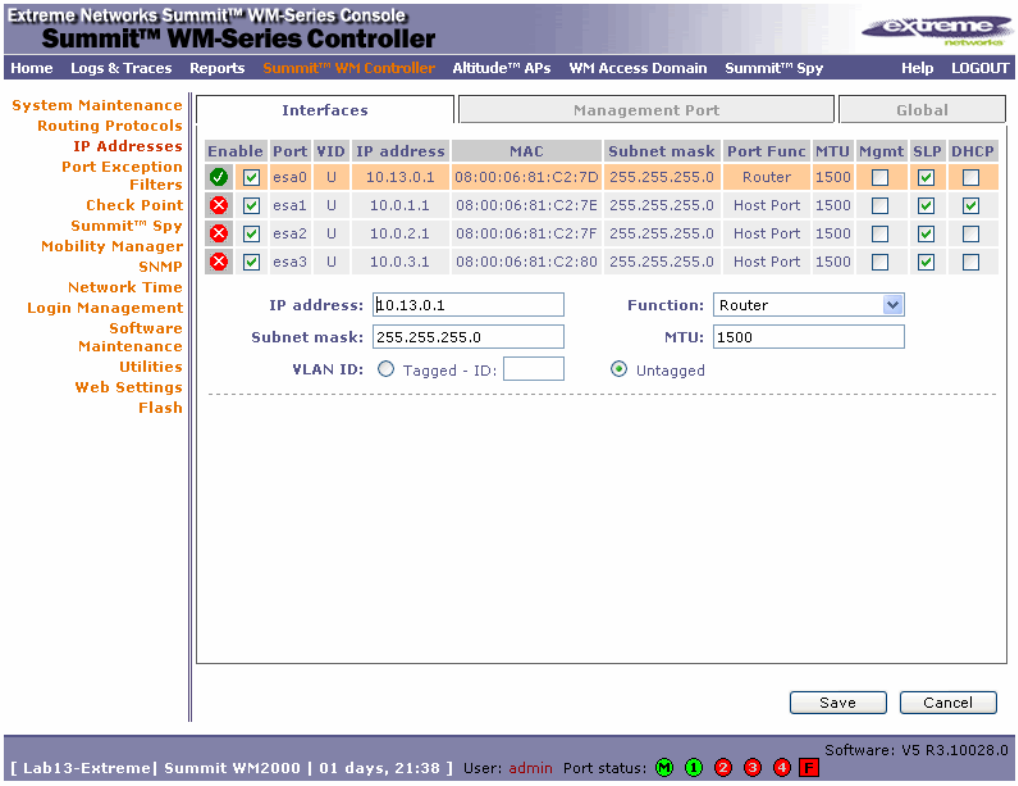
6 Click **Login**. The Summit WM GUI main menu page is displayed.

NOTE

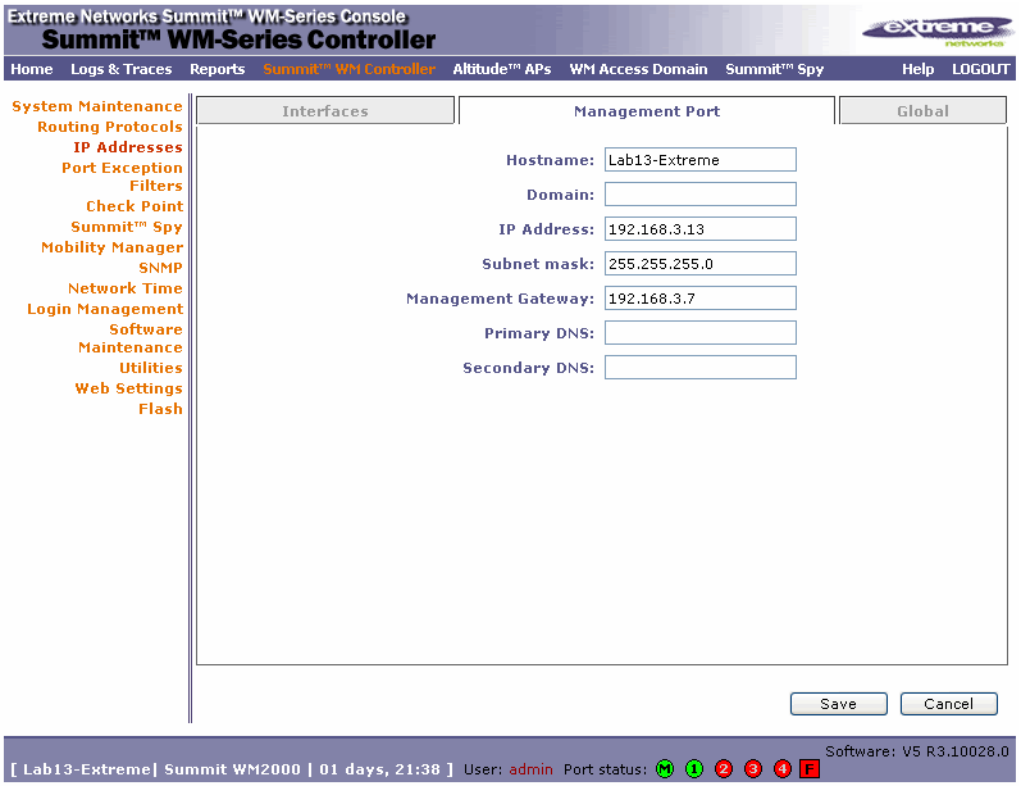
All images of the Summit WM GUI in this User Guide represent the Summit WM Controller WM200/2000. In the footer of the Summit WM GUI, the following is displayed:
- [host name | product name | up time]
For example, [WM | WM1000 | 02 days, 22:57][WM | WM200/2000 | 01 days, 04:15]. If your Summit WM GUI is running the WM200/2000 license, the footer will display WM200/2000.
- If there is no key (unlicensed), the product name will not be displayed.
*- **User** is the user id you used to login in. For example, admin.*
*- **Port Status** is the connectivity state of the port. M represents the Management interface, which is on eth0 and the numbered lights reflect the esa ports on the system. Green indicates the interface is up and running. Red indicates the interface is down. The F icon represents the flash drive status: green if the flash drive is mounted, and red if the flash drive is not mounted.*
- For the Summit WM Controller WM100, the footer of the Summit WM GUI does not include the link status of the physical interfaces.

7 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

8 In the left pane, click **IP Addresses**. The **Interfaces** page is displayed.



9 Click the **Management Port** tab. The **Management Port** page is displayed.



10 Type the following information:

- **Hostname** - Specifies the name of the Summit WM Controller
- **Domain** - Specifies the IP domain name of the enterprise network
- **IP Address** - Specifies the new IP address for the Summit WM Controller's management port. Change this as appropriate for the enterprise network.
- **Subnet mask** - Specifies the appropriate subnet mask for the IP address to separate the network portion from the host portion of the address (typically 255.255.255.0)
- **Management Gateway** - Specifies the default gateway of the network
- **Primary DNS** - Specifies the primary DNS server used by the network
- **Secondary DNS** - Specifies the secondary DNS server used by the network

11 To save your changes, click **OK.**

NOTE

The Web connection between the computer and the Summit WM Controller is now lost. The IP addresses are now set to the network you defined.

Changing the administrator password

It is recommended to change your default administrator password once your system is installed.

To change the administrator password:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Management Users**.

3 In the user_admin table, click **admin**.

4 In the **Modify User Password** box, type the new administrator password.

5 In the **Modify User Confirm Password** box, type the new administrator password again.

6 Click **Change Password**.

NOTE

The Summit WM Controller provides you with local login authentication mode and the RADIUS-based login authentication mode. The local login authentication is enabled by default. You can change the login authentication mode from local to RADIUS-based mode. For more information, see "Configuring the login authentication mode" on page 50.

Connecting the Summit WM Controller to your enterprise network

Once you have modified the management port configuration settings, the next step is to connect the Summit WM Controller to your enterprise network.

To connect the Summit WM Controller to your enterprise network:

1 Disconnect your computer from the Summit WM Controller management port.

2 Connect the Summit WM Controller management port to the enterprise Ethernet LAN.

3 Log on to the Summit WM GUI. The system is visible to the enterprise network.

Applying the product license key

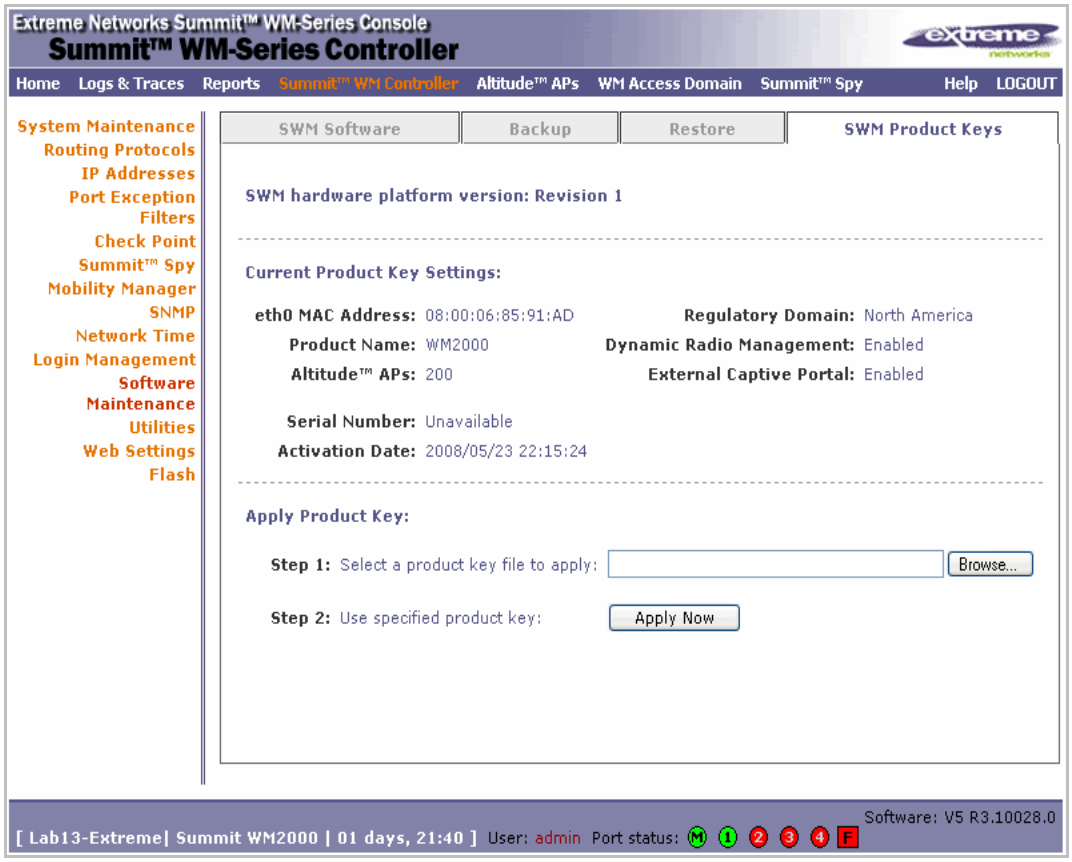
To ensure all available system functionality is enabled, your product license key must be applied.

To apply the product license key:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Software Maintenance**.

3 Click the **SWM Product Keys** tab.



4 In the **Apply Product Key** section, click **Browse** to navigate to the location of the product key file and click the file.

5 Click **Apply Now**. The product license key is applied, and the Summit WM Controller reboots.

Setting up the data ports

The next step in the initial setup of the Summit WM Controller is to configure the physical data ports.

A new Summit WM Controller is shipped from the factory with all its data ports set up as host ports. Support of management traffic is disabled on all data ports. Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states are enabled. A disabled interface does not allow data to flow (receive/transmit).

VLAN ID parameter

You can define a specific VLAN tag to be applied to a particular interface. All packets associated with that port will be tagged with the corresponding VLAN. This allows the Summit WM Controller to directly attach to a VLAN network without the need to remove VLAN tags at the connection port.

You can redefine the data ports to function as one of three types:

- **Host Port**

  Use a host port definition for connecting Altitude APs with no OSPF routing function on this port.

- **Third-Party AP Port**

  Use a third-party AP port definition for a port to which you will connect third-party APs. Only one port can be configured for third-party APs.

  Selecting this option prepares the port to support a third-party AP setup allowing the mapping of a WM-AD to the physical port. The WM-AD settings permit the definition of policy, such as filters and Captive Portal, which manage the traffic flow for wireless users connected to these APs.

  The third-party APs must operate as layer-2 bridges. The third-party AP WM-AD is isolated from the rest of the network. The Summit WM Controller assumes control over the layer-3 functions including DHCP.

- **Router Port**

  Use a router port definition for a port that you want to connect to a OSPF area to exchange routes to other OSPF routers.

  Altitude APs can be attached to a router port. The Summit WM Controller will create a virtual WM-AD port and handle wireless device traffic in the same manner as a host port.

NOTE

Third-party access points must not be directly connected to a router or host port.

There is a fourth port type that is not configurable in the Summit WM GUI:

- **WM Access Domain Services (WM-AD) interface**

  A WM-AD port is a virtual port created automatically on the Summit WM Controller when a new WM-AD is defined. The WM-AD port becomes the default gateway for wireless devices on this WM-AD. No Altitude APs can be associated with a WM-AD port and no routing is permitted on this port.

The chart below summarizes the port types and their functions:

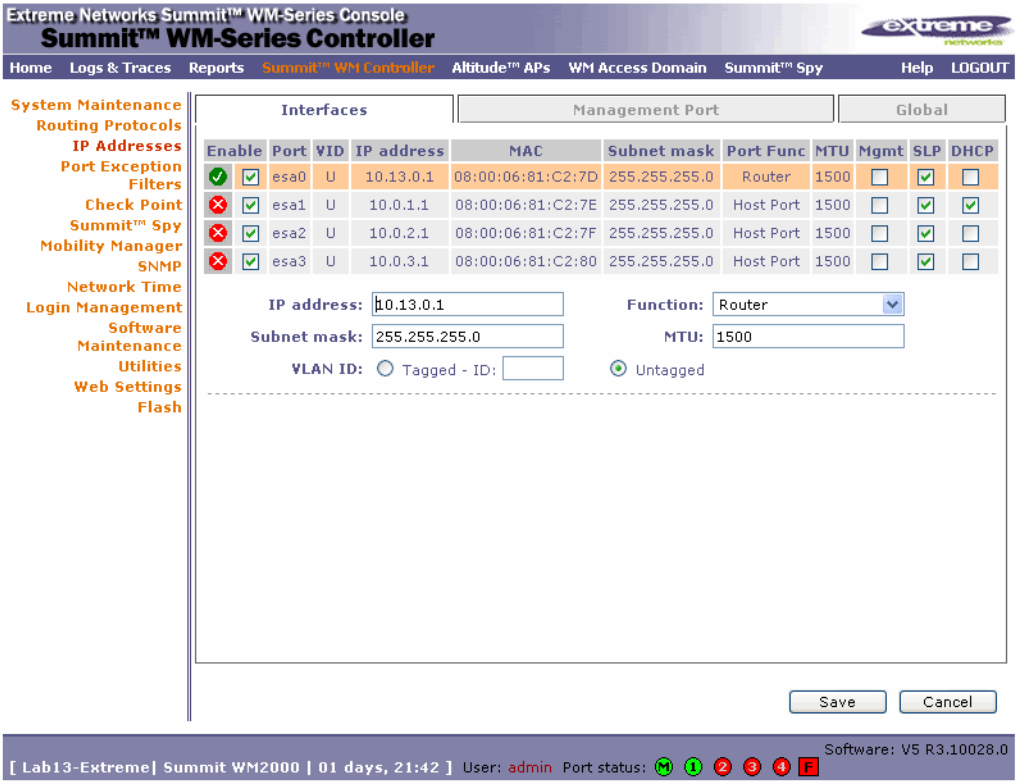
Table 2: Port types and functions

Port Type	Host	3rd-Party AP	Router	WM-AD
OSPF route advertisement	No	No	Selectable. Route wireless device traffic only.	No
Altitude AP support	Yes	No	Yes	No
Mgmt traffic support (SNMP, HTTP, TELNET, SLP, RADIUS, DHCP)	Selectable	Selectable	Selectable	Selectable
Routing protocol support (IP, OSPF and PIM)	No	No	Selectable	No

To configure the data port interfaces on the Summit WM Controller:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **IP Addresses**. The **Interfaces** page is displayed.



The upper portion of the **Interfaces** page displays the number of Ethernet ports of the Summit WM Controller:

- **Summit WM1000 Controller** - Two Ethernet ports
- **Summit WM100 Controller** - Four Ethernet ports
- **Summit WM200/2000 Controller** - Four Ethernet ports
- **Summit WM20 Controller** - Two Ethernet ports

NOTE

For the Summit WM100 Controller, the footer of the Summit WM GUI does not include the link status of the physical interfaces.

NOTE

All images of the Summit WM GUI in this User Guide represent the Summit WM200/2000 Controller.

3 Click a port.

Port configuration allows for the explicit state of the administration state for each interface. By default, data interface states are enabled. If they are not enabled, you can enable them each of them individually. A disabled interface does not allow data to flow (receive/transmit).

4 Type the following:

- **IP address** - The IP Address of the physical Ethernet port.
- **Subnet mask** - The appropriate subnet mask for the IP address, which separates the network portion from the host portion of the address (typically 255.255.255.0).
- **MTU** - The Maximum Transmission Unit or maximum packet size for this port. The default setting is 1500. If you change this setting and are using OSPF, be sure that the MTU of each port in the OSPF link matches.

NOTE

If the routed connection to an AP traverses a link that imposes a lower MTU than the default 1500 bytes, the Summit WM Controller and AP both participate in MTU discovery to automatically learn the correct MTU and adjust their settings accordingly. At the Summit WM Controller, MTU adjustments are tracked on a per AP basis.

5 In the **Function** drop-down list, click one of the following:

- **Host Port** - Specifies a port that will not participate in OSPF routing.
- **Third-Party AP Port** - Specifies a port that will communicate with third party access points.
- **Router Port** - Specifies a port that may participate in OSPF routing.

NOTE

For OSPF routing on a port, the port must be configured as a router port.

6 To enable management traffic, select the **Mgmt** checkbox. Enabling management provides access to SNMP (v2, get), SSH, and HTTPs management interfaces.

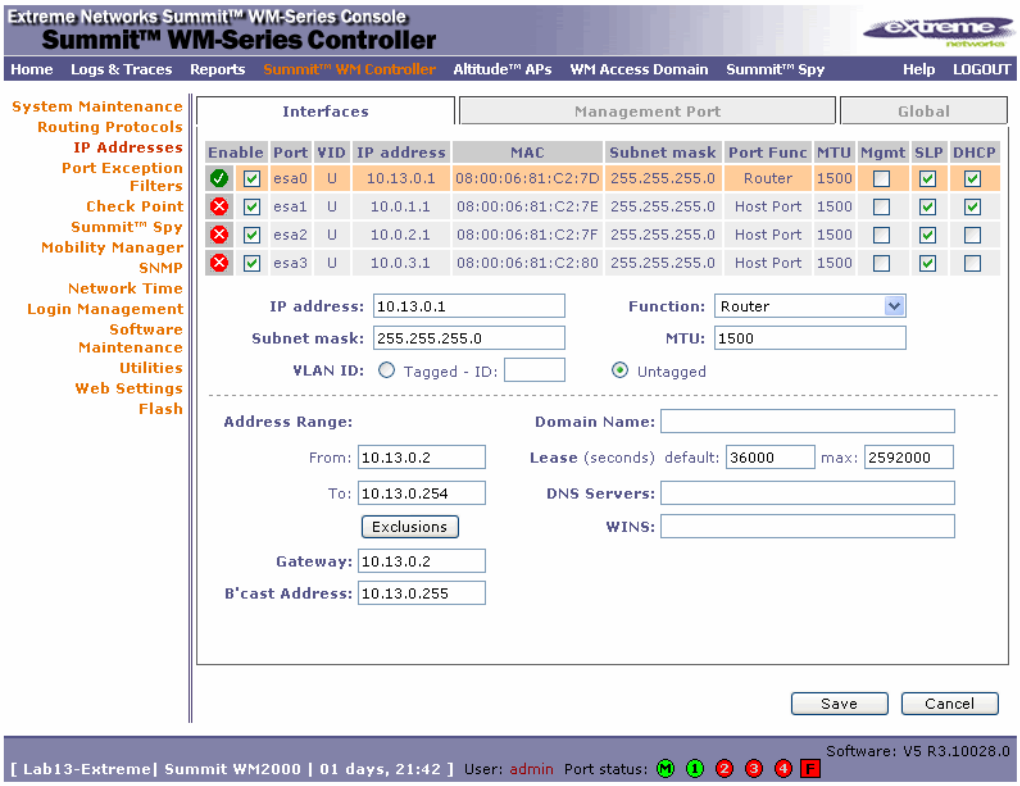
NOTE

This option does not override the built-in protection filters on the port.
The built-in protection filters for the port, which are restrictive in the types of packets that are allowed to reach the management plane, are extended with a set of definitions that allow for access to system management services through that interface (SSH, SNMP, HTTPS:5825).

7 To enable the SLP protocol, select the **SLP** checkbox.

Altitude APs use this port for discovery and registration. Other controllers can use this port to enable inter-controller device mobility if this port is configured to use SLP or the Summit WM Controller is running as a manager and SLP is the discovery protocol used by the agents.

8 To enable the local DHCP Server on the Summit WM Controller, select the **DHCP** box. The lower pane is populated with the DHCP's parameters.



NOTE

The local DHCP Server is useful as a general purpose DHCP Server for small subnets.

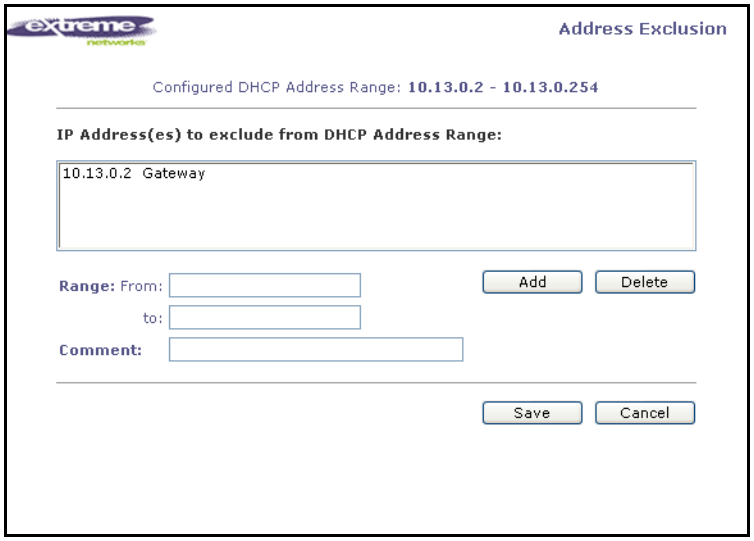
9 Type the following:

- In the **From** box, type the starting IP address of the IP address range from which the local DHCP Server will allocate the IP addresses to the Altitude APs.
- In the **To** box, type the ending IP address of the IP address range from which the local DHCP Server will allocate the IP addresses to the Altitude APs.

  Use the **Exclusion** button to exclude the IP addresses from allocation by the DHCP Server. The Summit WM Controller automatically includes the IP addresses of the Interfaces (Ports), and the default gateway in the exclusion list. You can not remove these IP addresses from the exclusion list.

  To exclude the IP addresses from allocation by the DHCP Server:

a Click on the Exclusion button. The DHCP Address Exclusion window opens.



b In the **From** box, type the starting IP address of the IP address range that you want to exclude from the DHCP allocation.

c In the **To** box, type the ending IP address of the IP address range that you want to exclude from the DHCP allocation.

NOTE

If you want to exclude just a single IP address from DHCP allocation, you must type the same IP address in the From and To boxes.

d In the **Comment** box, type any relevant comment. For example, you can type the reason for which a certain IP address is excluded from the DHCP allocation.

e Click on **Add**. The excluded IP addresses are displayed in the IP Address(es) to exclude from DHCP Range box.

f To delete a IP Address from the exclusion list, select it in the **IP Address(es) to exclude from DHCP Range** box, and then click **Delete**.

g To save your changes, click **Save**.

- In the **Gateway** box, type the IP address of the default gateway.

NOTE

Since the Summit WM Controller is not allowed to be the gateway for the Altitude APs, you cannot use the Interface IP address as the gateway address.

NOTE

The B'cast Address field is view only. This field is computed from the mask and the IP addresses.

- In the **Domain Name** box, type the name of the domain that you want the Altitude APs to use for DNS Server's discovery.
- In the **Lease (seconds) default** box, type the time period for which the IP address will be allocated to the Altitude APs.
- In the **Lease (seconds) max** box, type the maximum time period in seconds for which the IP address will be allocated to the Altitude APs.
- In the **DNS** box, type the DNS Server's IP address if you have the DNS Server.
- In the **WINS** box, type the WINS Server's IP address if you have the WINS Server.

NOTE

You can type multiple entries in DNS and WINS text boxes. Each entry must be separate by a comma. These two fields are not mandatory to be typed to enable the local DHCP feature.

10 To save your changes, click **Save**.

NOTE

When you deselect the DHCP checkbox, the DHCP fields disappear in the lower pane. When you again select the DHCP box, all the DHCP fields are again populated and visible.

Setting up Internal VLAN ID and multi-cast support for the ports

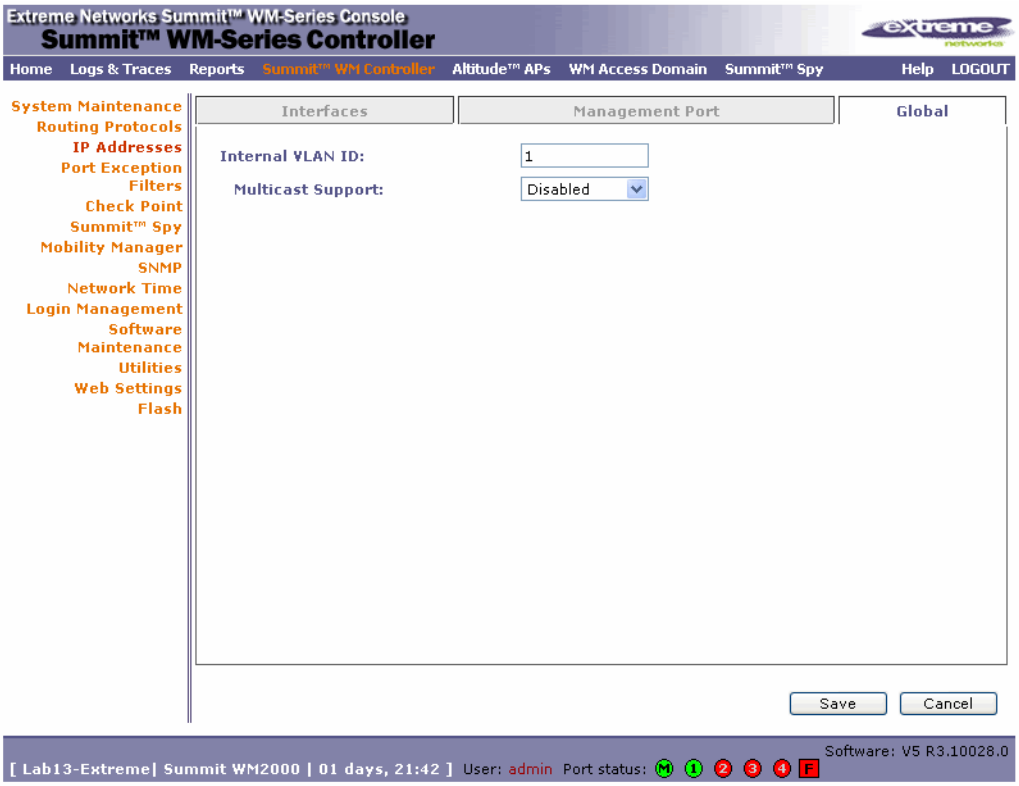
You can configure Internal VLAN ID, and enable multicast support for any of the data ports.

To configure the Internal VLAN ID and enable multicast support:

1 From the main menu, click **Wireless Controller Configuration**. The **Summit WM Controller Configuration** page is displayed.

2 In the left pane, click **IP addresses**. The **Interfaces** page is displayed.

3 Click the **Global** tab. The **Global** page is displayed.



4 In the **Internal VLAN ID** box, type the internal VLAN ID.

5 From the **Multicast Support** drop-down list, click the port: esa0, esa1, esa2 and esa3esa0 or esa1.

6 To save your changes, click **Save**.

Setting up static routes

It is recommended that you define a default route to your enterprise network, either with a static route or by using OSPF protocol. A default route enables the Summit WM Controller to forward packets to destinations that do not match a more specific route definition.

To set a static route on the Summit WM Controller:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.

3 To add a new route, in the **Destination Address** box type the destination IP address of a packet. To define a default static route for any unknown address not in the routing table, type **0.0.0.0**.

4 In the **Subnet Mask** box, type the appropriate subnet mask to separate the network portion from the host portion of the IP address (typically 255.255.255.0). To define the default static route for any unknown address, type 0.0.0.0.

5 In the **Gateway** box, type the IP address of the specific router port or gateway on the same subnet as the Summit WM Controller to which to forward these packets. This is the IP address of the next hop between the Summit WM Controller and the packet's ultimate destination.

6 Click **Add**. The new route is added to the list of routes.

7 Select the **Override dynamic routes** checkbox to give priority over the OSPF learned routes, including the default route, which the Summit WM Controller uses for routing. This option is enabled by default.

To remove this priority for static routes, so that routing is controlled dynamically at all times, clear the **Override dynamic routes** checkbox.

NOTE

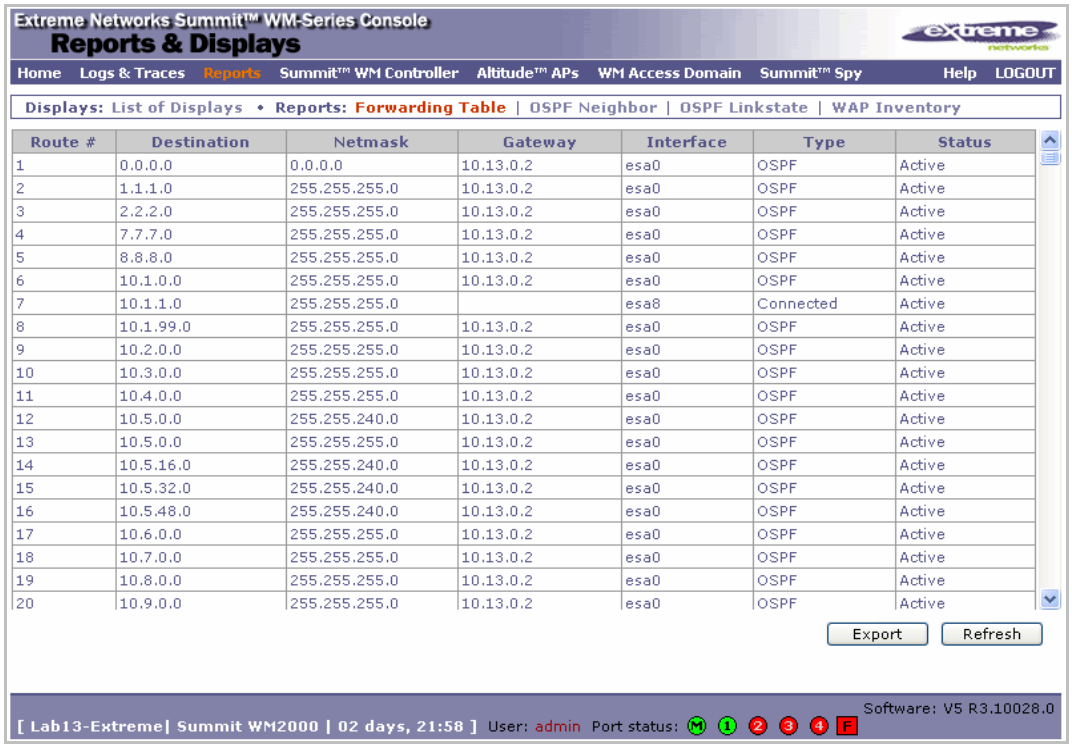
If you enable dynamic routing (OSPF), the dynamic routes will normally have priority for outgoing routing. For internal routing on the Summit WM Controller, the static routes normally have priority.

8 To save your changes, click **Save**.

To view the forwarding table on the Summit WM Controller:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 To view the static routes that have been defined for the Summit WM Controller, click **Forwarding Table**. The **Forwarding Table** is displayed.


Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Route # Destination Netmask Gateway Interface Type Status
1 0.0.0.0 0.0.0.0 10.13.0.2 esa0 OSPF Active
2 1.1.1.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
3 2.2.2.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
4 7.7.7.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
5 8.8.8.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
6 10.1.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
7 10.1.1.0 255.255.255.0 esa8 Connected Active
8 10.1.99.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
9 10.2.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
10 10.3.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
11 10.4.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
12 10.5.0.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
13 10.5.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
14 10.5.16.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
15 10.5.32.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
16 10.5.48.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
17 10.6.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
18 10.7.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
19 10.8.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
20 10.9.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
Export
Refresh
Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 02 days, 21:58] User: admin Port status: M 1 2 3 4 F

This report displays all defined routes, whether static or OSPF, and their current status.

3 To update the display, click **Refresh**.

Setting up OSPF Routing

To enable OSPF (OSPF RFC2328) routing, you must:

- Define one data port as a router port in the **IP Addresses** page
- Enable OSPF globally on the Summit WM Controller
- Define the global OSPF parameters
- Enable (or disable) OSPF on the port that you defined as a router port

Ensure that the OSPF parameters defined here for the Summit WM Controller are consistent with the adjacent routers in the OSPF area. This consistency includes the following:

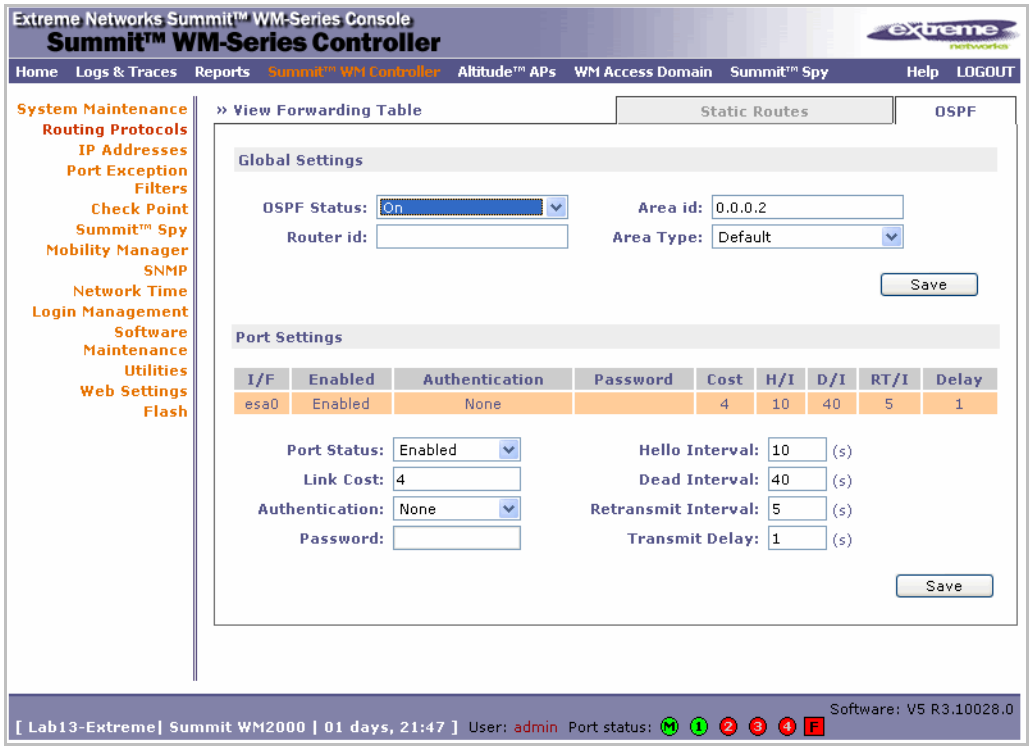
- If the peer router has different timer settings, the protocol timer settings in the Summit WM Controller must be changed to match, in order to achieve OSPF adjacency.
- The MTU of the ports on either end of an OSPF link must match. The MTU for ports on the Summit WM Controller is defined as 1500, on the **IP Addresses** page, during data port setup. This matches the default MTU in standard routers.

To set OSPF Routing Global Settings on the Summit WM Controller:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Routing Protocols**. The **Static Routes** tab is displayed.

3 Click the **OSPF** tab.



4 From the **OSPF Status** drop-down list, click **On** to enable OSPF.

5 In the **Router ID** box, type the IP address of the Summit WM Controller. This ID must be unique across the OSPF area. If left blank, the OSPF daemon automatically picks a router ID from one of the Summit WM Controller's interface IP addresses.

6 In the **Area ID** box, type the area. 0.0.0.0 is the main area in OSPF.

7 In the **Area Type** drop-down list, click one of the following:

- **Default** - The default acts as the backbone area (also known as area zero). It forms the core of an OSPF network. All other areas are connected to it, and inter-area routing happens via a router connected to the backbone area.
- **Stub** - The stub area does not receive external routes. External routes are defined as routes which were distributed in OSPF via another routing protocol. Therefor, stub areas typically rely on a default route to send traffic routes outside the present domain.
- **Not-so-stubby** - The not-so-stubby area is a type of stub area that can import autonomous system (AS) external routes and send them to the default/backbone area, but cannot receive AS external routes from the backbone or other areas.

8 To save your changes, click **Save**.

To set OSPF Routing Port Settings on the Summit WM Controller:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Routing Protocols**.

3 Click the **OSPF** tab. The **OSPF Settings** page is displayed.

4 In the **Port Status** drop-down list, click **Enabled** to enable OSPF on the port. The default setting is **Disabled**.

5 In the **Link Cost** box, type the OSPF standard for your network for this port. This is the cost of sending a data packet on the interface. The lower the cost, the more likely the interface is to be used to forward data traffic. The default setting is **10** for WM100/WM1000.

NOTE

If more than one port is enabled for OSPF, it is important to prevent the Summit WM Controller from serving as a router for other network traffic (other than the traffic from wireless device users controlled by the Summit WM Controller). To ensure that the Summit WM Controller is never the preferred OSPF route, set the Link Cost to its maximum value of 65535. Filters should also be defined that will drop routed packets. For more information, see "Configuring filtering rules for a WM-AD" on page 181.

6 In the **Authentication** drop-down list, click the authentication type for OSPF on your network: **None** or **Password**. The default setting is **None**.

7 If **Password** is selected as the authentication type, in the **Password** box, type the password. If **None** is selected as the Authentication type, leave this box empty. This password must match on either end of the OSPF connection.

8 Type the following:

- **Hello-Interval** - Specifies the time in seconds (displays OSPF default).The default setting is 10 seconds.
- **Dead-Interval** - Specifies the time in seconds (displays OSPF default). The default setting is **40** seconds.
- **Retransmit-Interval** - Specifies the time in seconds (displays OSPF default). The default setting is **5** seconds.
- **Transmit Delay** - Specifies the time in seconds (displays OSPF default). The default setting is **1** second.

9 To save your changes, click **Save**.

To confirm that ports are set for OSPF:

1 To confirm that the ports are set up for OSPF, and that advertised routes from the upstream router are recognized, click **View Forwarding Table**. The **Forwarding Table** is displayed.

The following additional reports display OSPF information when the protocol is in operation:

- **OSPF Neighbor** - Displays the current neighbors for OSPF (routers that have interfaces to a common network)
- **OSPF Linkstate** - Displays the Link State Advertisements (LSAs) received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies.

2 To update the display, click **Refresh**.

Filtering at the interface level

The Summit WM solution has a number of built-in filters that protect the system from unauthorized traffic. These filters are specific only to the Summit WM Controller. These filters are applied at the network interface level and are automatically invoked. By default, these filters provide stringent-level rules to allow only access to the system's externally visible services. In addition to these built-in filters,

the administrator can define specific exception filters at the interface-level to customize network access. These filters do not depend on a WM-AD definition.

Built-in port-based exception filters

On the Summit WM Controller, various port-based exception filters are built in and invoked automatically. These filters protect the Summit WM Controller from unauthorized access to system management functions and services via the ports. Access to system management functions is granted if the administrator selects the **allow management** option.

Allow management traffic is now specific to the interface being allowed. For example, if allow management is allowed on a physical port (esa0), only users connected through ESA0 will be able to get access to the system. Users connecting on any other interface such as a WM-AD (esa6) will no longer be able to target ESA0 to gain management access to the system. In order to allow access for users connected on a WM-AD, the WM-AD configuration itself must have **allow management** enabled and users will only be able to target the WM-AD interface specifically.

NOTE

You can also enable management traffic in the WM-AD definition.

For example, on the Summit WM Controller's data interfaces (both physical interfaces and WM-AD virtual interfaces), the built-in exception filter prohibits invoking SSH, HTTPS, or SNMP. However, such traffic is allowed, by default, on the management port.

If management traffic is explicitly enabled for any interface (physical port or WM-AD), access is implicitly extended to that interface through any of the other interfaces (WM-AD). Only traffic specifically allowed by the interface's exception filter is allowed to reach the Summit WM Controller itself. All other traffic is dropped. Exception filters are dynamically configured and regenerated whenever the system's interface topology changes (for example, a change of IP address for any interface).

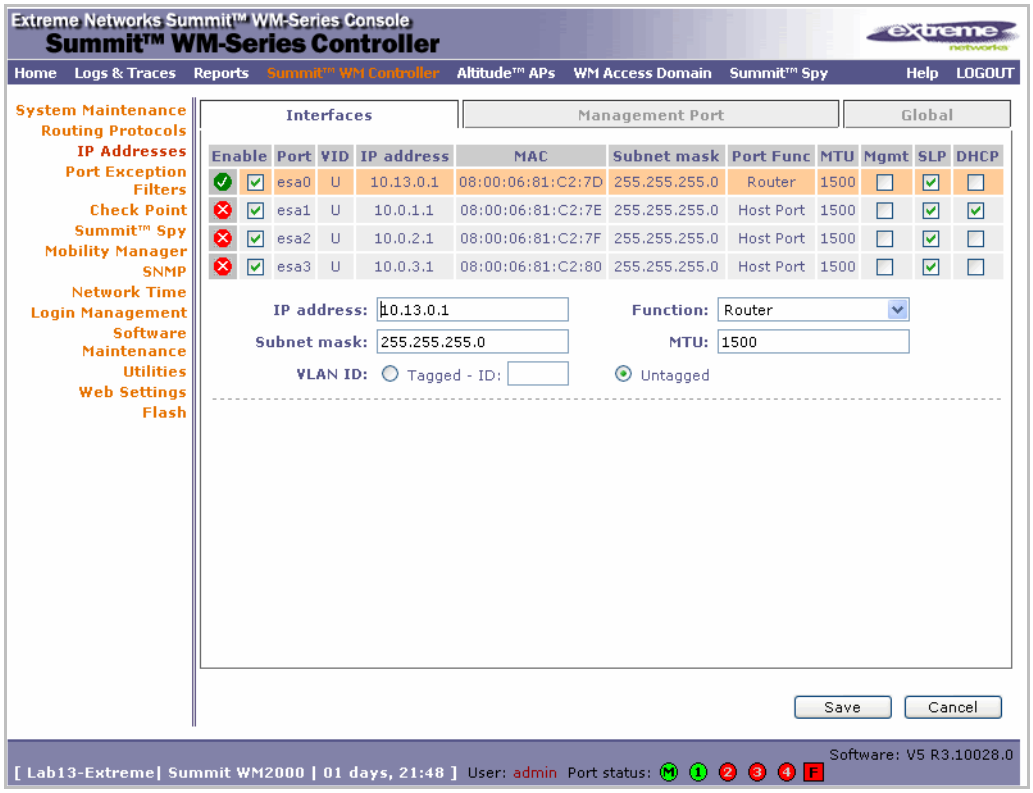
Enabling management traffic on an interface adds additional rules to the exception filter, which opens up the well-known IP(TCP/UDP) ports, corresponding to the HTTPS, SSH, and SNMP applications.

The port-based built-in exception filtering rules, in the case of traffic from WM-AD users, are applicable to traffic targeted directly for the WM-ADs interface. For example, a WM-AD filter may be generic enough to allow traffic access to the Summit WM Controller's management (for example, Allow All [*.*.*.*]). Exception filter rules are evaluated after the user's WM-AD assigned filter policy, as such, it is possible that the WM-AD policy allow the access to management functions that the exception filter denies. These packets are dropped.

To enable SSH, HTTPS, or SNMP access through a data interface:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **IP Addresses**. The **Interfaces** page is displayed.



3 On the **Interfaces** page, click the appropriate interface.

4 Select the corresponding **Management** checkbox.

5 To save your changes, click **Save**.

User defined port-based exception filters

You can add specific filtering rules at the port level in addition to the built-in rules. Such rules give you the capability of restricting access to a port, for specific reasons, such as a Denial of Service (DoS) attack.

The filtering rules are set up in the same manner as filtering rules defined for a WM-AD - specify an IP address and then either allow or deny traffic to that address. For more information, see "Configuring filtering rules for a WM-AD" on page 181.

The rules defined for port exception filters are prepended to the normal set of restrictive exception filters and have precedence over the system's normal protection enforcement.

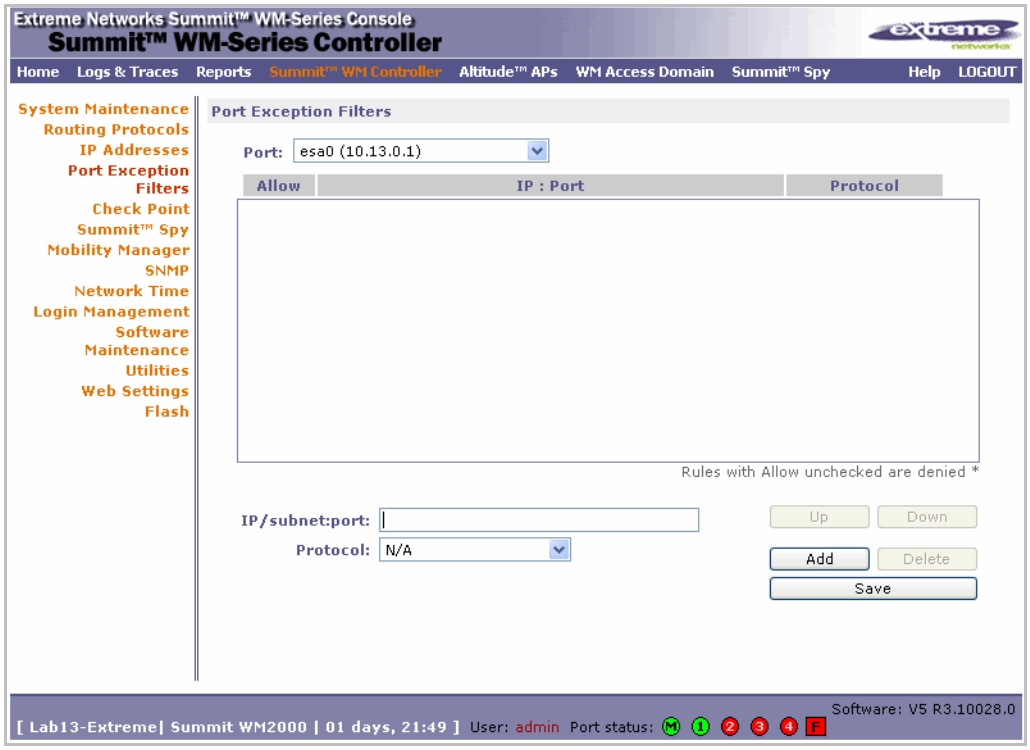
WARNING!

If defined improperly, user exception rules may seriously compromise the systems normal security enforcement rules. They may also disrupt the system's normal operation and even prevent system functionality altogether. It is advised to only augment the exception-filtering mechanism if absolutely necessary.

To define port exception filters:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Port Exception Filters**. The **Port Exception Filters** page is displayed.



3 In the **Port** drop-down list, click the applicable data port.

4 In the **IP / subnet: port** box, type the destination IP address. You can also specify an IP range, a port designation or a port range on that IP address.

5 In the **Protocol** drop-down list, click the protocol you want to specify for the filter. This list may include **UDP**, **TCP**, **IPsec-ESP**, **IPsec-AH**, **ICMP**. The default is N/A.

6 Click **Add**. The new filter is displayed on the **Filter** section of the page.

7 Click the new filter.

8 To allow traffic, select the **Allow** checkbox.

9 To adjust the order of the filtering rules, click **Up** or **Down** to position the rule. The filtering rules are executed in the order defined here.

10 To save your changes, click **Save**.

Configuring the login authentication mode

You can configure either the local login authentication mode, or the RADIUS login authentication mode to authenticate the user's login attempts. While the local login authentication mode uses locally configured login and passwords, the RADIUS login authentication mode uses the RADIUS Server to authenticate the users' login attempts.

NOTE

The Summit WM software enables you to recover the Summit WM Controller via the Rescue mode if you have lost its login password. For more information, see the Summit WM Maintenance Guide.

Configuring the local login authentication mode and adding new users

The local login authentication mode is enabled by default. If the login authentication was previously set to RADIUS authentication mode, you can change it to the local authentication.

You can also add new users and define their access rights - whether administrative or read only.

To configure the local login authentication mode:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen appears.

2 From the left pane, click **Login Management**. The **Login Management** screen appears.

3 In the **Authentication mode** section, select **Local**.

4 In the **Add User** section, select one of the following:

- **user_admin** - Grants the administrator's access rights to the user.
- **user_read** - Grants the 'read only' access right to the user.

5 In the **User ID** box, type the user's ID.

6 In the **Password** box, type the user's password.

NOTE

The password must be eight to 24 characters long.

7 In the **Confirm Password** box, re-type the password.

8 To add the user, click **Add User**. The new user is added and the user's ID appears under the **user_admin** column.

Configuring the RADIUS login authentication mode

The local login authentication mode is enabled by default. You can change the local login authentication mode to RADIUS-based authentication.

NOTE

Before you change the default local login authentication to RADIUS-based authentication, you must configure the RADIUS Server on the Global Settings screen. For more information, see "WM-AD global settings" on page 149.

RADIUS is a client/server authentication and authorization access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response it receives from one or more RADIUS servers. RADIUS uses User Datagram Protocol (UDP) for sending the packets between the RADIUS client and server.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key

to encrypt all RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

NOTE

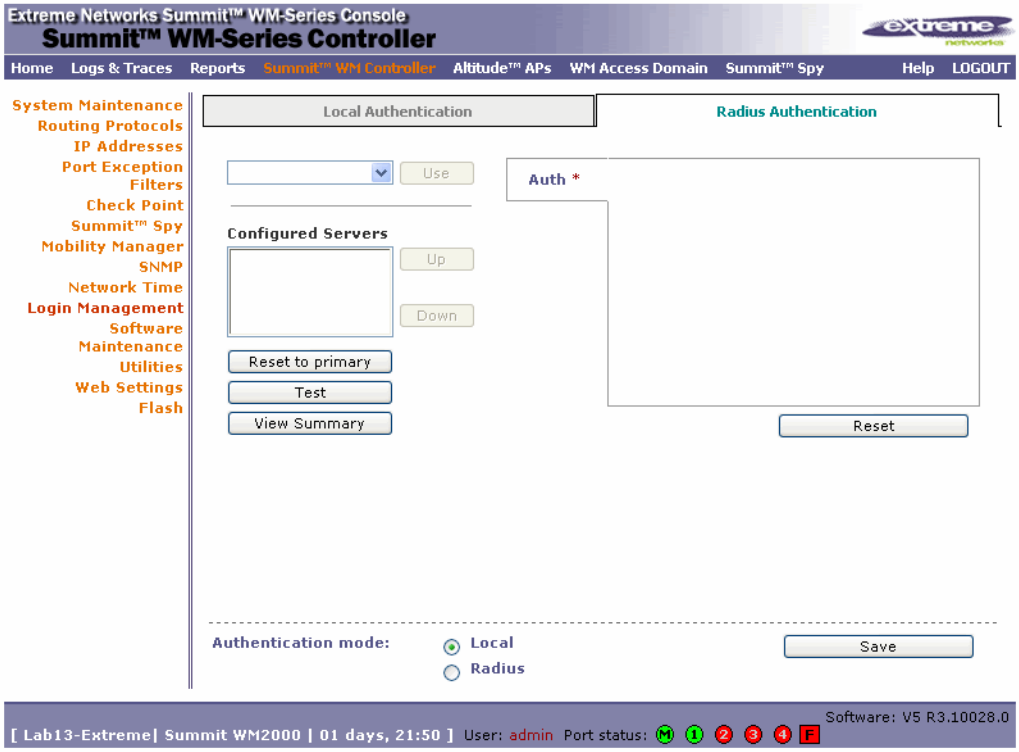
Before you configure the system to use RADIUS-based login authentication, you must configure the Service-Type RADIUS attribute on the RADIUS server. For more information, see the RADIUS-based login authentication section in the Summit WM Technical Reference Guide.

To configure the RADIUS login authentication mode:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen appears.

2 From the left pane, click **Login Management**. The **Login Management** screen appears.

3 Click the **RADIUS Authentication** tab. The **RADIUS Authentication** screen appears



4 In the **Authentication mode** section, select **Radius**.

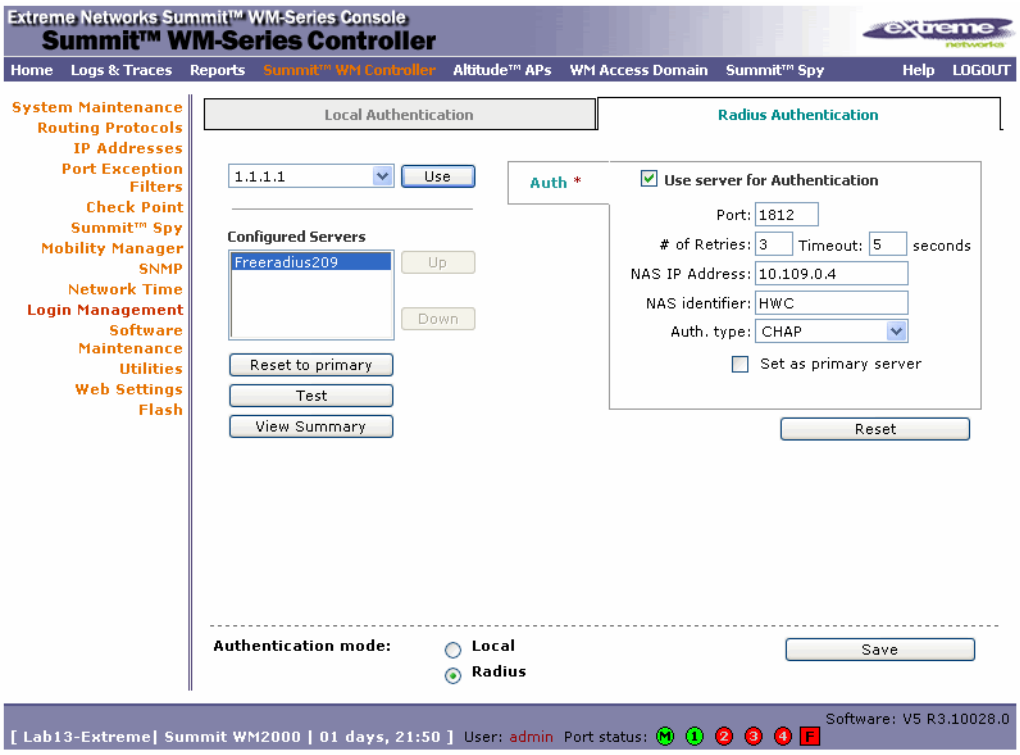
5 From the menu, located next to the **Use** button, select the RADIUS Server that you want to use for the RADIUS login authentication, and then click Use. The RADIUS Server's name is displayed in the **Configured Servers** box, and in the **Auth** section, and the following default values of the RADIUS Server are displayed.

NOTE

The RADIUS Serves displayed in the menu, located against the Use button, are defined on Global Settings screen. For more information, see "WM-AD global settings" on page 149.

- **Port #** - The port number of the RADUS Server.
- **# of Retries** - Number of times the Summit WM Controller tries to connect to the RADIUS Server if the RADIUS Timeout interval is exceeded.
- **Timeout** - Number of seconds the Summit WM Controller waits for a response from the RADIUS Server before declaring timeout.
- **NAS IP address** - The IP address of Network Access Server (NAS).
- **NAS Identifier** - The Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers, and then acting on the response returned.
- **Auth Type** - The authentication protocol type, whether PAP or CHAP.
- **Set as Primary Server** - Specifies the Primary RADIUS Server when there are multiple RADIUS servers.

You can modify any of the aforesaid values.

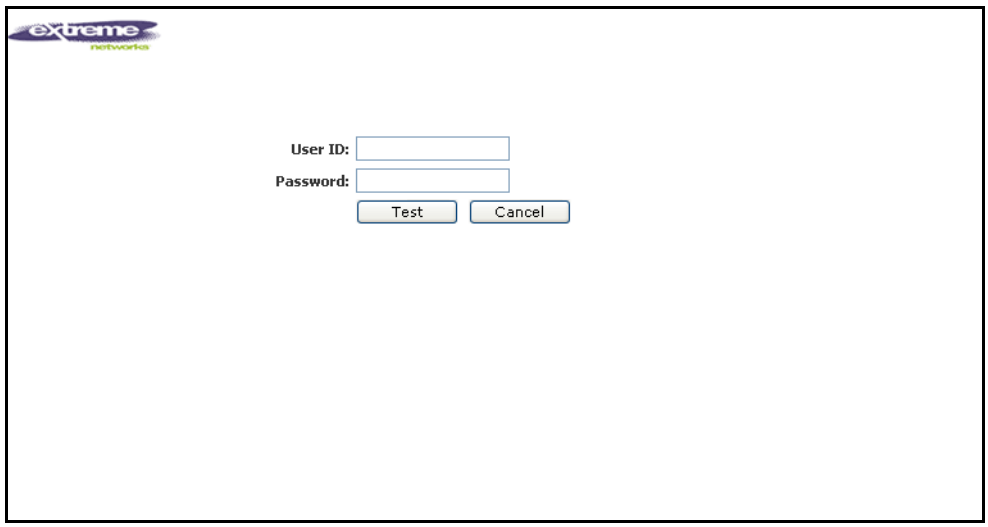


6 To add additional RADIUS servers, repeat Step 5.

NOTE

You can add up to three RADIUS servers to the list of login authentication servers. When you add two or more RADIUS Servers to the list, you must designate one of them as the Primary server. The Summit WM Controller first attempts to connect to the Primary Server. If the Primary Server is not available, it tries to connect to the second and third server according to their order in the Configured Servers box. You can change the order of RADIUS servers in the Configured Servers box by clicking on the Up and Down buttons.

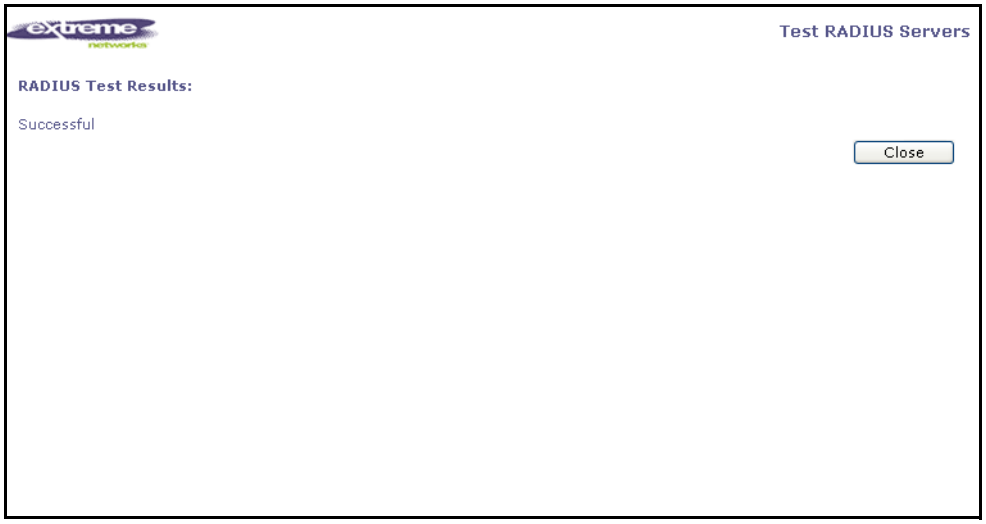
7 To test the RADIUS Server's login configuration, click on **Test**. The following window appears.



8 In the **User ID** and the **Password** boxes, type the user's ID and the password, which were configured on the RADIUS Server, and then click **Test**. The RADIUS connectivity result is displayed.

NOTE

To learn how to configure the User ID and the Password on the RADIUS Server, refer to your RADIUS Server's user guide.



NOTE

After configuring the RADIUS-based login authentication mode, you must always test the connectivity to RADIUS Server as explained in Step 6 and 7. If you do not test the RADIUS Server connectivity, and you have made some error in configuring the RADIUS-based login authentication mode, you will be locked out of the Summit WM Controller.

NOTE

If the RADIUS connectivity test displays "successful" result, you must click Save on the RADIUS Authentication screen (as depicted in Step 4) to save your configuration. After you save your changes, you will be logged out of the Summit WM Controller. You must use the RADIUS login user name and password to log on the Summit WM Controller.

Configuring network time

You can synchronize the network elements to a universal clock. This ensures accuracy in usage logs. Network time is synchronized in one of two ways:

- Using system time
- Using Network Time Protocol (NTP), an Internet standard protocol that synchronizes client workstation clocks.

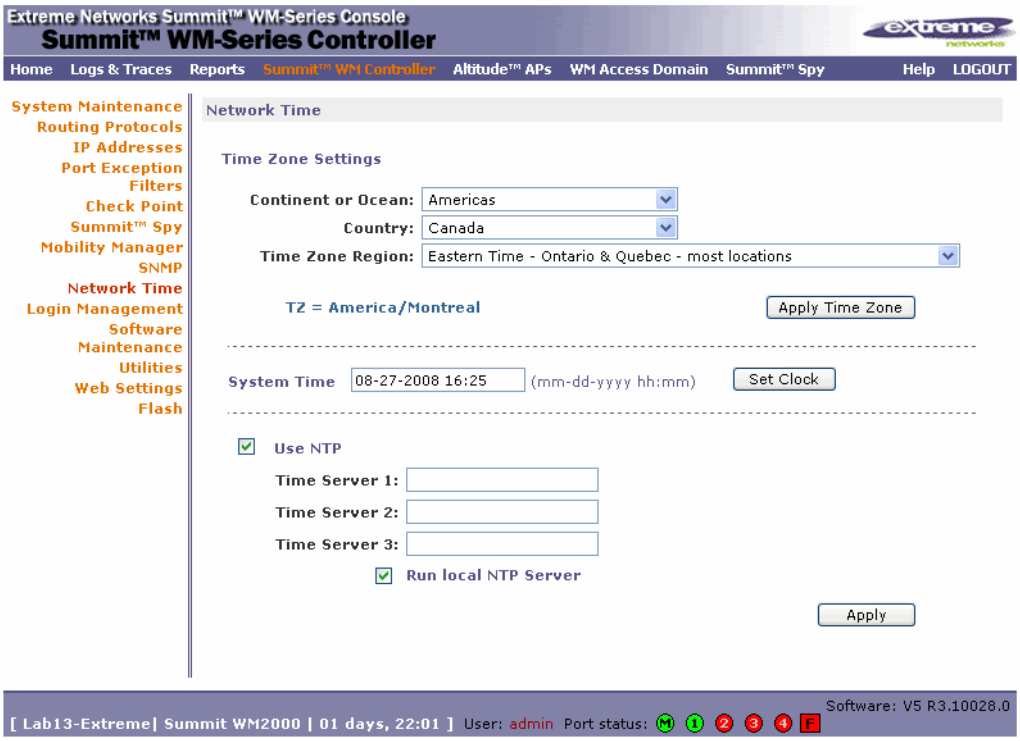
NOTE

If the Summit WM Controller is left powered-down for more than 78 hours, its capacitor dies down and is unable to keep the system clock working. In such a case, you must synchronize the network time, using the NTP server. If the NTP server is not reachable, you must first manually set the system to the correct time, and then use the system time to synchronize the network time.

To apply time zone settings:

1 From the main menu, click **Wireless Controller Configuration**. The Wireless Controller Configuration page is displayed.

2 In the left pane, click **Network Time**. The **Network Time** page is displayed.



3 From the **Continent or Ocean** drop-down list, click the appropriate large-scale geographic grouping for the time zone.

4 From the **Country** drop-down list, click the appropriate country for the time zone. The contents of the drop-down list change based on the selection in the **Continent or Ocean** drop-down list.

5 From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.

6 To apply your changes, click **Apply Time Zone.**

To set system time parameters:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** page is displayed.

2 In the left pane, click **Network Time**. The **Network Time** page is displayed.

3 To use system time, select the **Use System Time** radio button.

4 Type the time setting in the **Use System Time** box, using the mm-dd-yyyy hh:mm format.

5 To apply your changes, click **Apply.**

To set Network Time Protocol:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** page is displayed.

2 In the left pane, click **Network Time**. The **Network Time** page is displayed.

3 To use Network Time Protocol, select the **Use NTP** option.

4 In the **Use System Time** box, type the time setting using the mm-dd-yyyy hh:mm format.

5 In the **Time Server 1** box, type the IP address or FQDN of a standard NTP Time Server. You can repeat this step for the **Time Server 2** and **Time Server 3** boxes.

NOTE

If any of the Time Servers is not accessible, you can use the Summit WM Controller as the Time Server. To use the Summit WM Controller as the Time Server, select the Run local NTP Server checkbox. When you select the Run local NTP Server checkbox, the time on the network elements is synchronized on the basis of the Summit WM Controller's system clock.

6 To apply your changes, click **Apply**.

Completing the system configuration

Once you have performed the initial configuration of the Summit WM Controller, you are now ready to do the following:

- **Configuring the WM-AD** - For more information, see Chapter 4, "WM Access Domain Services."
- **Registering and assigning APs to the WM-AD** - For more information, see Chapter 3, "Configuring the Altitude AP."

Ongoing Operations of the Controller, Access Points, and WM software

Once you have configured the WM-AD and registered and assigned APs to the WM-AD, the Controller, Access Points, and WM software system configuration is complete. Ongoing operations of the Controller, Access Points, and WM software system can include the following:

- Summit WM Controller System Maintenance
- Altitude AP Maintenance
- Client Disassociate
- Logs and Traces
- Reports and Displays

For more information, see "Performing system administration" on page 297 or the *Summit WM Maintenance Guide*.

3 Configuring the Altitude AP

This chapter discusses the Altitude AP, the Controller, Access Points, and WM software solution, including:

- "Altitude AP overview" on page 59
- "Discovery and registration overview" on page 71
- "Configuring the Altitude APs for the first time" on page 80
- "Adding and registering an Altitude AP manually" on page 83
- "Configuring Altitude AP settings" on page 84
- "Modifying an Altitude AP's properties based on a default AP configuration" on page 134
- "Modifying the Altitude AP's default setting using the Copy to Defaults feature" on page 134
- "Configuring Altitude APs simultaneously" on page 135
- "Performing Altitude AP software maintenance" on page 137

Altitude AP overview

The Altitude AP is a wireless LAN access point that uses the 802.11 wireless standards (802.11a/b/g/n) for network communications. The Altitude AP bridges network traffic to an Ethernet LAN. The Altitude AP is provided with proprietary software that allows it to communicate only with the Summit WM Controller.

The Altitude AP physically connects to a LAN infrastructure and establishes an IP connection to the Summit WM Controller. The Altitude AP has no user interface - instead the Altitude AP is managed through the Summit WM GUI. The Altitude AP's configuration is centrally managed and applied from the Summit WM Controller. In addition, the Summit WM Controller provides centralized management (verification and upgrade) of the Altitude AP firmware image.

All communication with the Summit WM Controller is carried out using a UDP-based protocol, which encapsulates IP traffic from the Altitude AP and directs it to the Summit WM Controller. The Summit WM Controller decapsulates the packets and routes them to the appropriate destinations, while managing sessions and applying policy.

The Altitude AP comes in the following variants:

- Altitude AP
- Outdoor AP (Siemens brand of outdoor AP)
- Altitude 802.11n AP

NOTE

The term, 'Altitude AP', is used in this document to encompass all three variants - Altitude AP, Outdoor AP (Siemens), and Altitude 802.11n AP. The variants are only specifically identified in the documentation where it is necessary to do so.

Altitude AP

The Altitude AP is meant for indoor environments. It can be mounted on walls or ceilings, using special brackets, and can be kept completely out of sight.

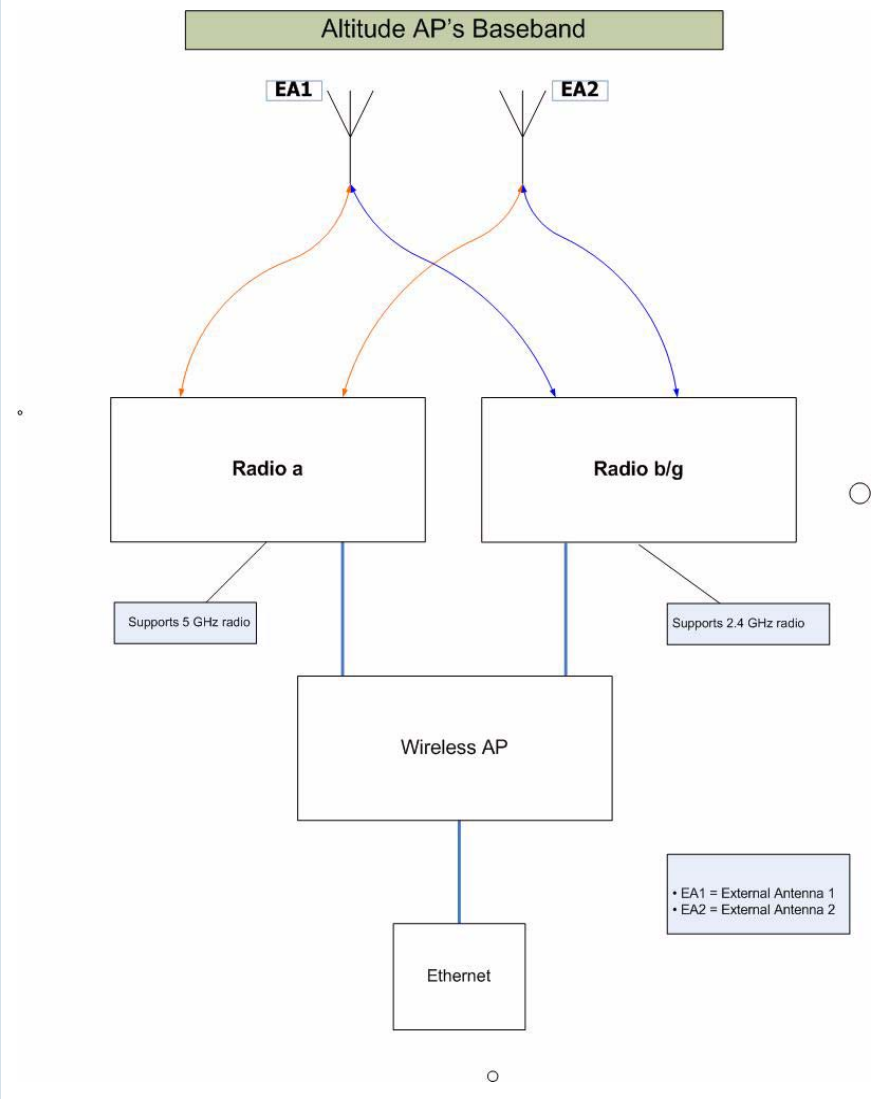
The Altitude AP is available in the following models:

- **Altitude 350-2i** - Internal antenna, internal dual (multimode) diversity antennas
- **Altitude 350-2d** - External antenna (dual external antennas), RP-SMA connectors

Altitude AP radios

The Altitude AP is equipped with two radios - radio **11a** and radio **11b/g**. The following is a block diagram of the Altitude AP equipped with external antennas.

Figure 4: Altitude AP block diagram



The Figure 4 illustrates the following:

- The Altitude AP has two radios - 11**a** radio and 11**b/g** radio.
- The 11**a** radio supports 5 GHz radio
- The 11**b/g** radio supports 2.4 GHz radio
- The 11**a** radio and the 11**b/g** radio are connected to both the external antennas - EA1 and EA2.

5 GHz radio supporting the 802.11a standard - The 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5-GHz band. The 802.11a standard uses an orthogonal frequency division multiplexing encoding scheme, rather than Frequency-Hopping Spread Spectrum (FHSS) or Direct-Sequence Spread Spectrum (DSSS).

2.4 GHz radio supporting the 802.11b/g standards - The 802.11g standard applies to wireless LANs and specifies a transmission rate of 54 Mbps. The 802.11b (High Rate) standard is an extension to 802.11 that specifies a transmission rate of 11 Mbps. Since 802.11g uses the same communication frequency range as 802.11b (2.4 GHz), 802.11g devices can co-exist with 802.11b devices on the same network.

The radios are enabled or disabled through the Summit WM GUI. Both radios can be enabled to offer service simultaneously. For more information, see "Topology of a WM-AD" on page 143.

The Unlicensed National Information Infrastructure (U-NII) bands are three frequency bands of 100 MHz each in the 5 GHz band, designated for short-range, high-speed, wireless networking communication.

The Altitude AP supports the full range of 802.11a:

- 5.15 to 5.25 GHz - U-NII Low Band
- 5.25 to 5.35 GHz - U-NII Middle Band
- 5.47 to 5.725 GHz - UNII 2+
- 5.725 GHz to 5.825 GHz Band - U-NII High Band

Outdoor AP

The Siemens-branded outdoor AP (OAP) can be managed by Summit WM controller. The following models of Siemens-branded Outdoor APs are managed by Summit WM. These are dual radio 11a/b/g access points designed for outdoor and harsh environment use.

- SEN 2650 (Internal antennas)
- SEN 2660 (External antennas)
- A&D W786-2HPW (Internal antennas with Ethernet)
- A&D W786-2HPW (Internal antennas with Fiber Optic)
- A&D W786-2HPW (External antennas with Ethernet)
- A&D W786-2HPW (External antennas with Fiber Optic)

The Outdoor AP enables you to extend your Wireless LAN beyond the confines of indoor locations. They are resistant to harsh outdoor conditions and extreme temperatures. Using the advanced wireless distribution feature of the Summit WM LAN, the Outdoor AP can extend your Wireless LAN to outdoor locations without Ethernet cabling. A mounting bracket is available to enable quick and easy mounting of the Outdoor APs to walls, rails, and poles.

The Outdoor AP supports the 802.11a, 802.11g, and full backward compatibility with legacy 802.11b devices.

NOTE

The Outdoor AP can also be deployed in indoor environments.

NOTE

The configuration process is identical for Altitude APs, Outdoor APs, and Altitude 802.11n APs, unless specified otherwise.

NOTE

The radio specifications of the Outdoor AP is identical to the Altitude AP. For more information, see "Altitude AP radios" on page 60

Altitude 802.11n AP

The Altitude 802.11n AP is an IEEE 802.11n (draft)-compliant access point that offers significant increase in data throughput and coverage range without additional bandwidth or transmit power. With both 2.4 GHz and 5 GHz 802.11n (draft) standard radio modules, the Altitude 802.11n AP delivers total data rates of up to 300 Mbps. Given that the improved throughput of 300 Mbps will be spread over a number of simultaneous users, the performance of the Altitude 802.11n AP will be close to that of a wired 100 Mbps Ethernet connection - the standard for desktop connectivity. With the Altitude 802.11n AP, mobile users get a similar experience to wired networks while accessing high-bandwidth data, voice, and video applications.

The Wireless 802.11n AP can achieve link rates of up to 300 Mbps. To achieve this high link rate, specific items need to be configured through the Summit WM Graphical User Interface. For more information, see "Achieving high throughput with the Wireless 802.11n AP" on page 102.

NOTE

The Altitude 802.11n AP is backward-compatible with existing 802.11a/b/g networks.

NOTE

The Altitude 802.11n AP cannot operate as a stand-alone access point.

MIMO

The mainstay of 802.11 AP is MIMO (multiple input, multiple output) - a technology that uses advanced signal processing with multiple antennas to improve the throughput. MIMO takes the advantage of multipath propagation to decrease packet retries to improve the fidelity of the wireless network.

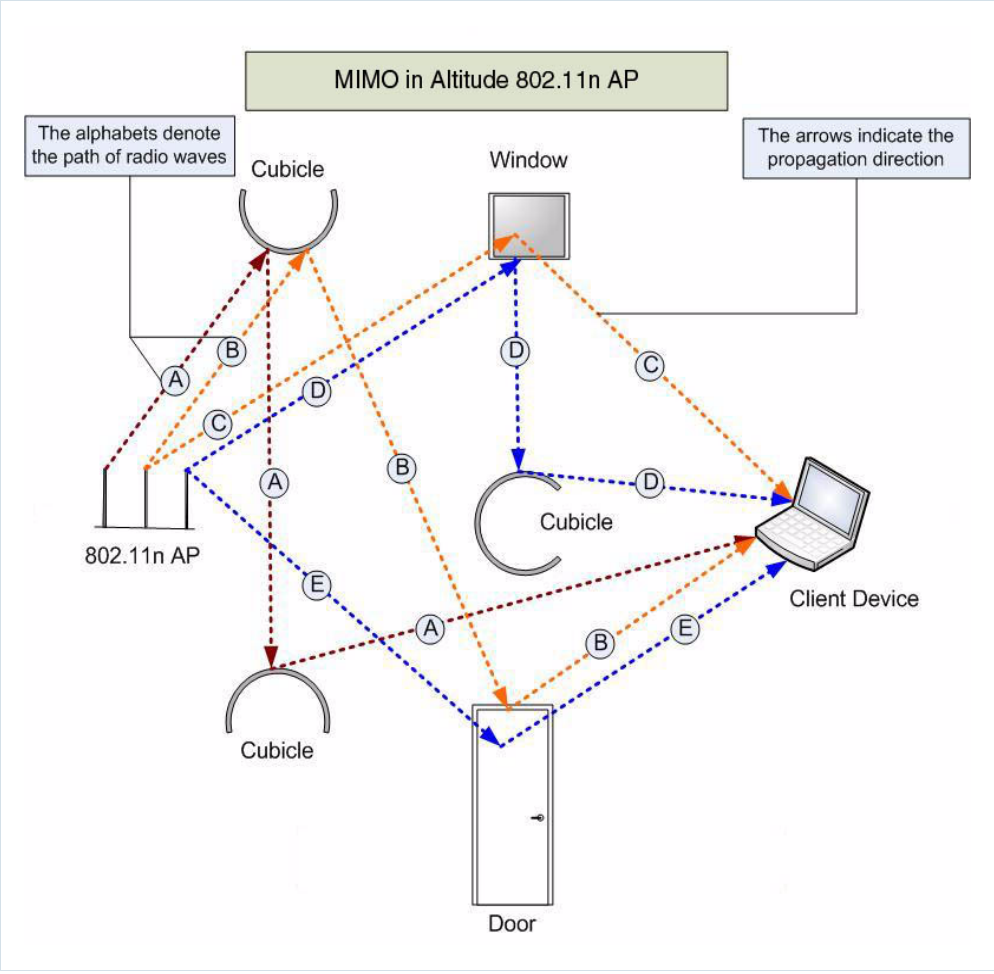
The 802.11n AP's MIMO radio sends out one or two radio signals through its three antennas. Each of these signals is called a spatial stream. Because the location of the antennas on the 802.11n AP is spaced out, each spatial stream follows a slightly different path to the client device. Furthermore, the three spatial streams get multiplied into several streams as they bounce off the obstructions in the vicinity.

This phenomenon is called multipath. Since these streams are bounced from different surfaces, they follow different paths to the client device. The client device, which is also 802.11n compliant, also has multiple antennas. Each of the antennas independently decodes the arriving signal. Then each antenna's decoded signal is combined with the decoded signals from the other antennas. The software algorithm, uses the redundancy to extract one or two spatial streams and enhances the streams' "signal to noise ratio".

The client device too sends out one or two spatial streams through its multiple antennas. These spatial streams get multiplied into several steams as they bounce off the obstructions in the vicinity enroute to 802.11n AP. The 802.11n AP's MIMO receiver receives these multiple streams with three antennas. Each of the three antennas independently decodes the arriving signal. Then each antenna's decoded signal is combined with the decoded signals from the other antennas. The 802.11n AP's MIMO receiver again uses the redundancy to extract one or two spatial streams and enhances the streams' "signal to noise ratio".

By using the multiple streams, MIMO doubles the throughput.

Figure 5: MIMO in Altitude 802.11n AP



NOTE

*MIMO should not be confused with the **Diversity** feature. While **Diversity** is the use of two antennas to increase the odds that a better radio stream is received on either of the antennas, MIMO antennas radiate and receive multi-*

streams of the same packet to achieve the increased throughput.
*The **Diversity** feature is meant to offset the liability of RF corruption, arising out of multipath, whereas MIMO converts the liability of multipath to its advantage.*

Because the 802.11n AP operates with multiple-antennas, it is capable of picking up even the weakest signals from the client devices.

Channel bonding

In addition to MIMO technology, the 802.11n AP makes a number of additional changes to the radio to increase the effective throughput of the Wireless LAN. The radios of regular Altitude APs use radio channels that are 20 MHz wide. This means that the channels must be spaced at 20 MHz to avoid interference. The radios of 802.11n AP can use two channels at the same time to create a 40 MHz wide channel. By using the two 20 MHz channels in this manner, the 802.11n AP achieves more than double throughput. The 40-MHz channels in 802.11n are two adjacent 20-MHz channels, bonded together. This technique of using two channels at the same time is called channel bonding.

Shortened guard interval

The purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections of symbols in orthogonal frequency division multiplexing (OFDM) - a method by which information is transmitted via a radio signal in Altitude APs.

In OFDM method, the beginning of each symbol is preceded by a guard interval. As long as the echoes fall within this interval, they will not affect the safe decoding of the actual data, as data is only interpreted outside the guard interval. Longer guard periods reduce the channel efficiency. The 802.11n AP provides reduced guard periods, thereby increasing the throughput.

MAC enhancements

The 802.11n AP also has an improved MAC layer protocol that reduces the overheads (in the MAC layer protocol) and the contention losses. This results in increased throughput.

The 802.11n AP is available in the following two models:

- **Altitude 450** - Six internal antennas
- **Altitude 451** - Three external antennas

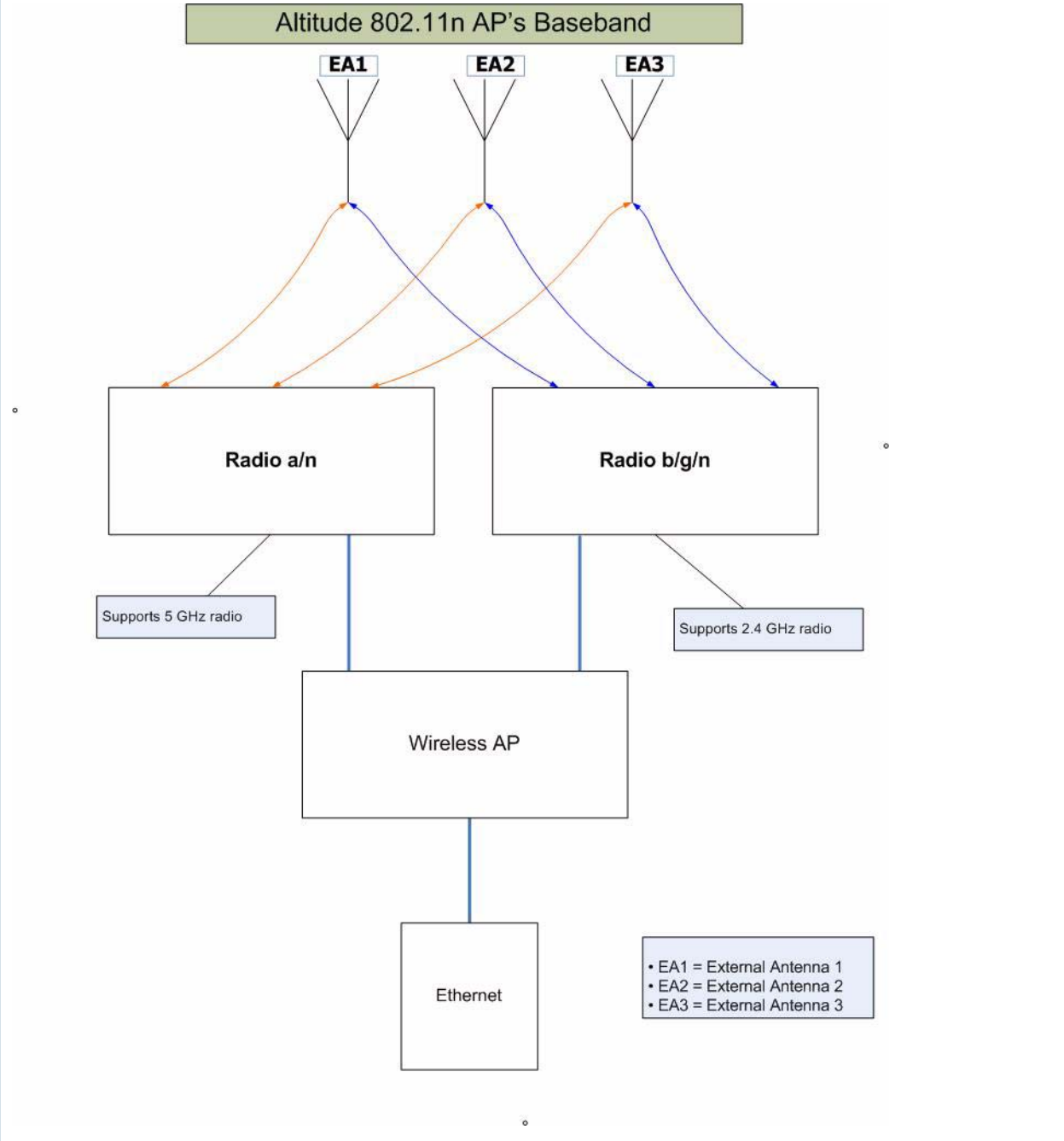
NOTE

The 802.11n AP cannot be deployed in an outdoor environment.

Altitude 802.11n AP's radios

The Altitude 802.11n AP is equipped with two radios - radio **a/n** and radio **b/g/n**. The following is a block diagram of the Altitude 802.11n AP equipped with external antennas.

Figure 6: Altitude 802.11n AP block diagram



The Figure 6 illustrates the following:

- The Altitude 802.11n AP has two radios - **11a/n radio** and **11b/g/n radio**.
- Both the radios are connected to all three antennas - EA1, EA2 and EA3.
- The **11a/n radio** supports 5 GHz radio
- The **11b/g/n radio** supports 2.4 GHz radio

5 GHz radio supporting the 802.11a/n standard - When in legacy 802.11a mode, the Altitude 450/451 AP supports data rates up to 54Mbps identical to the Altitude 350-2i/350-2d AP. The modulation used

is OFDM. In 802.11n mode there are 2 supported channel bandwidths, 20MHz and 40MHz. The 802.11n AP supports up to 300Mbps in 40MHz channels and 130Mbps in 20MHz channels. The modulation used is 3x3 MIMO (multiple input, multiple output).

2.4 GHz radio supporting the 802.11b/g/n standard - When in legacy 802.11b/g mode, the Altitude 450/451 AP supports data rates up to 54Mbps identical to the Altitude 350-2i/350-2d AP. The modulation used is OFDM for 11g and CCK for 11b. In 802.11n mode there are 2 supported channel bandwidths, 20MHz and 40MHz. The Altitude 450/451 AP supports up to 300Mbps in 40MHz channels and 130Mbps in 20MHz channels. The modulation used is 3x3 MIMO (multiple input multiple output).

The radios are enabled or disabled through the Summit WM GUI. For more information, see "Modifying Altitude 802.11n AP 450/451 radio properties" on page 90.

The Unlicensed National Information Infrastructure (U-NII) bands are three frequency bands of 100 MHz each in the 5 GHz band, designated for short-range, high-speed, wireless networking communication.

The 802.11n AP supports the full range of frequencies available in the 5GHz band:

- 5150 to 5250 MHz - U-NII Low band
- 5250 to 5350 MHz - U-NII middle band
- 5470 to 5700 MHz - U-NII Worldwide
- 5725 to 5825 MHz - U-NII high band

NOTE

The Wireless 802.11n AP can achieve link rates of up to 300Mbps. To achieve this level of high link rates, specific items need to be configured through the Summit WM GUI. For more information, see "Modifying Altitude 802.11n AP 450/451 radio properties" on page 90.

Altitude AP default IP address and first-time configuration

The Altitude APs are shipped from the factory with a default IP address - 192.168.1.20. The default IP address simplifies the first-time IP address configuration process for Altitude APs. The Altitude AP returns to its default IP address if the Altitude AP is not successful in its discovery process, which determines the IP address of the Altitude AP and of the Summit WM Controller. Altitude AP behavior ensures that only one Altitude AP at a time on a subnet can use the default IP address. For more information, see "Discovery and registration overview" on page 71.

Altitude AP LEDs indicate when it is possible to connect the Altitude AP using the default IP address. For more information, see "Understanding the Altitude AP LED status" on page 73.

Altitude APs can have their IP addresses assigned using two methods, either a Dynamic Host Configuration Protocol (DHCP) server assigns the IP address or an administrator can assign the IP address using the static configuration option. The DCHP IP address assignment method is the default method for Altitude AP configuration. The Altitude AP returns to its default IP address assignment if the DHCP assignment is not successful. DHCP assignment is part of the discovery process. For more information, see "Discovery and registration overview" on page 71. The Altitude AP default IP address impacts the first-time configuration processes for both methods:

- **DHCP server** - If successful, the Altitude AP is assigned an IP address by the network's DHCP server when the Altitude AP is powered on.
  - If the DHCP assignment is not successful in the first 60 seconds, the Altitude AP returns to its default IP address.

- The Altitude AP waits for 30 seconds in default IP address mode before attempting again to acquire the IP address from the DHCP.
- The process repeats itself until the DHCP assignment is successful, or until an administrator assigns the Altitude AP an IP address using static configuration.

NOTE

You can telnet the Altitude AP during the 30 seconds the Altitude AP is assigned its default IP address. If a static IP address is assigned during this period, you must reboot the Altitude AP for the configuration to take effect.

- **Static configuration** - You can assign a static IP address to the Altitude AP. For more information, see the following section.

Assigning static IP address to Altitude AP

In order to establish the telnet session, you have to ping the Altitude AP's IP address. You must know the correct IP address to ping. The Altitude AP's IP address may have the default values or the DHCP-assigned values, depending upon the network condition. The concept is explained with the help of the following network conditions:

DHCP server is available on the network

The Altitude AP gets the IP address via the DHCP assignment, and successfully discovers the controller.

- If the Altitude AP gets the IP address via the DHCP assignment and it successfully discovers the controller, you can configure its static IP address via the controller's user interface. For more information, see "Setting up the Altitude AP using static configuration" on page 114.

The Altitude AP gets the IP address via the DHCP assignment, but fails to discover the controller.

- Ping the IP address that is assigned to the Altitude AP via the DHCP assignment.

DHCP server is not available on the network

The DHCP server is not available on the network, and the Altitude AP reverts to its factory defaults after trying for 60 seconds to get the IP address via the DHCP assignment.

- Ping the default IP address.

NOTE

The default IP address of all the Altitude AP variants - Altitude AP, Outdoor AP and the Altitude 802.11n AP - is 192.168.1.20.

To assign the static IP address to the Altitude AP:

1 Connect the Altitude AP to network.

2 Ping the Altitude AP's IP address.

3 When the ping is successful, telnet the Altitude AP.

NOTE

If the telnet session is not established within 30 seconds of successful pinging, the Altitude AP again initiates the process of getting the IP address via the DHCP assignment.

The default user name and the password for telnet access are:

- User Name - **admin**
- Password - **new2day**

You can override the default password by setting up a new telnet access password on the Altitude Registration screen. For more information see "Enabling/Disabling telnet access and setting up new Telnet Access Password via the controller's user interface" on page 69.

4 Configure the static configuration, using the following CLI commands.

CLI commands for configuring static IP address in the Altitude AP:

The CLI commands to configure the static IP address in the Altitude AP and the Outdoor APs are identical.

Syntax.

```
set <dhcp disable>
set <ipaddr>
set <ipmask>
```

Parameters.

Table 3: *CLI command to configure static IP address in the Altitude AP*

Parameter Name	Description
dhcp disable	By default, the Altitude AP is configured to acquire its IP address via the DHCP assignment. The command disables the DHCP server.
ipaddr	Specifies the static IP address.
ipmask	Specifies the subnet

NOTE

After you run these commands, you must reboot the Altitude AP for the configuration to take effect.

CLI commands to configure static IP address in the Altitude 802.11n AP:

Syntax.

```
cset <dhcp disable>
cset <ipaddr>
cset <ipmask>
cset <gateway>
capply
csave
```

Parameters.

Table 4: *CLI command to configure static IP address in the Altitude 802.11n AP*

Parameter Name	Description
dhcp disable	By default, the Altitude AP is configured to acquire its IP address via the DHCP assignment. The command disables the DHCP server.
ipaddr	Specifies the IP address.
ipmask	Specifies the subnet.
gateway	Specifies the IP address of the network gateway.
capply	Applies the configuration.
csave	Saves the configuration.

NOTE

After you run these commands, you must reboot the Altitude 802.11n AP for the configuration to take effect.

Enabling/Disabling telnet access and setting up new Telnet Access Password via the controller's user interface

You can enable/disable the telnet access, and set up a new Telnet Access Password via the controller's user interface. The Altitude AP must successfully discover the controller to pick up this configuration.

NOTE

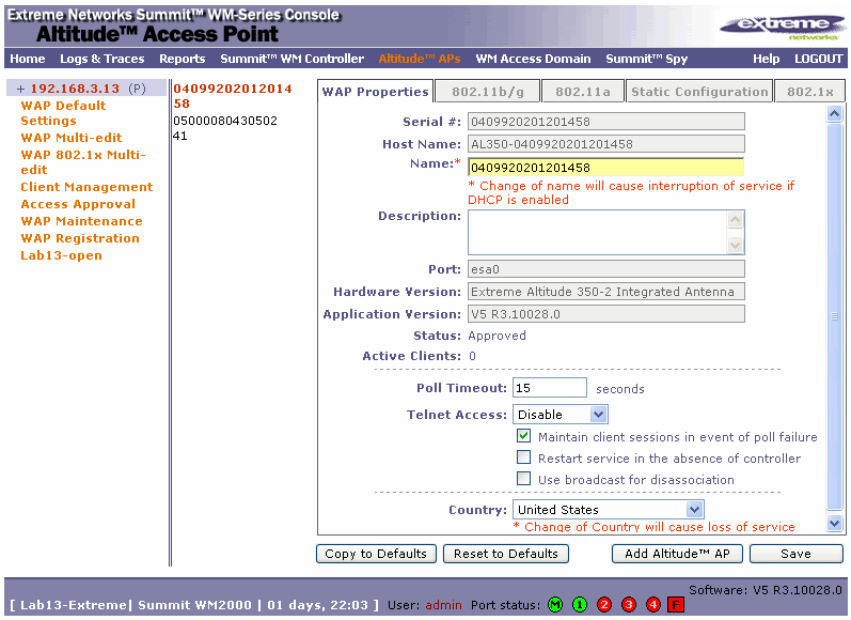
The new telnet access password that you set up over the controller's user interface overrides the default telnet access password.

Enabling/disabling telnet access via the controller's user interface

To enable/disable telnet access:

1 From the main menu, click Altitude AP Configuration. The Altitude AP Configuration screen appears.

2 In the Altitude AP list, click the Altitude AP for which you want to enable/disable telnet.



3 From the Telnet Access drop-down menu, select Enable to enable the telnet access, or select Disable to disable the telnet access.

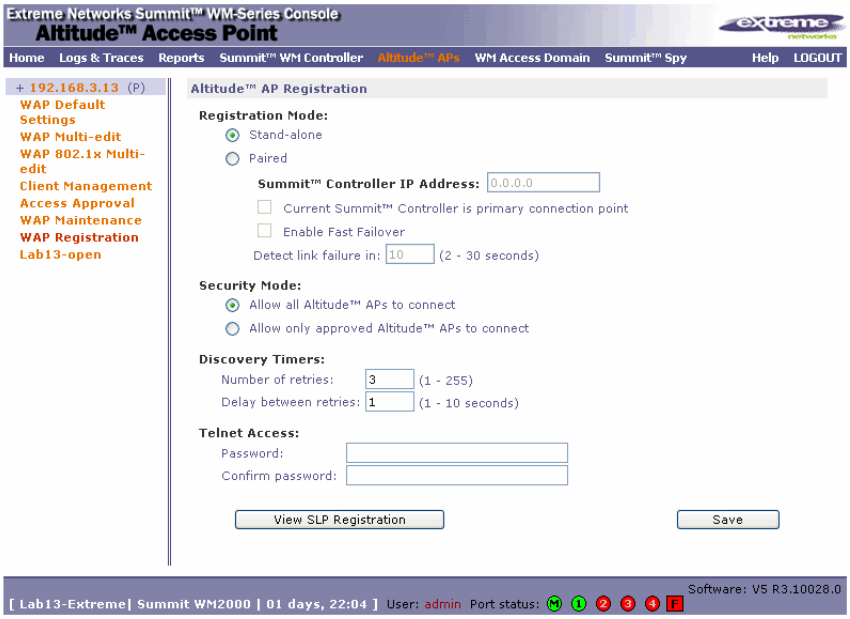
4 Click Save.

Setting up a new Telnet Access Password via the controller's user interface

To set up a new Telnet Access Password:

1 From the main menu, click Altitude AP Configuration. The Altitude AP Configuration screen appears.

2 From the left pane, click AP Registration. The Altitude AP Registration screen appears.


Extreme Networks Summit™ WM-Series Console
Altitude™ Access Point
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
+ 192.168.3.13 (P)
WAP Default Settings
WAP Multi-edit
WAP 802.1x Multi-edit
Client Management
Access Approval
WAP Maintenance
WAP Registration
Lab13-open
Altitude™ AP Registration
Registration Mode:
Stand-alone
Paired
Summit™ Controller IP Address: 0.0.0.0
Current Summit™ Controller is primary connection point
Enable Fast Failover
Detect link failure in: 10 (2 - 30 seconds)
Security Mode:
Allow all Altitude™ APs to connect
Allow only approved Altitude™ APs to connect
Discovery Timers:
Number of retries: 3 (1 - 255)
Delay between retries: 1 (1 - 10 seconds)
Telnet Access:
Password:
Confirm password:
View SLP Registration
Save
Software: V5 R3.10028.0
[Lab13-Extreme] Summit WM2000 | 01 days, 22:04] User: admin Port status:

3 Under the **Telnet Access** section, type the new password in the **Password** box.

4 In the **Confirm Password** box, retype the password.

5 Click **Save**.

Discovery and registration overview

When the Altitude AP is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the Summit WM Controller. When the discovery process is successful, the Altitude AP registers with the Summit WM Controller.

WARNING!

Only use power supplies that are recommended by Extreme Networks.

Altitude AP discovery

Altitude APs discover the IP address of a Summit WM Controller using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the Altitude AP successfully locates a Summit WM Controller to which it can register.

You must ensure that the appropriate services on your enterprise network are prepared to support the discovery process. The following five steps summarize the discovery process:

- **Step 1 - Use the IP address of the last successful connection to a Summit WM Controller.**

  Once a Altitude AP has successfully registered with a Summit WM Controller, it recalls that controller's IP address, and uses that address on subsequent reboots. The Altitude AP bypasses discovery and goes straight to registration.

  If this discovery method fails, it cycles through the remaining steps until successful.

- **Step 2 - Use the predefined static IP addresses for the Summit WM Controllers on the network (if configured).**

  You can specify a list of static IP addresses of the Summit WM Controllers on your network. On the **Static Configuration** tab, add the addresses to the **Wireless Controller Search List**.

  CAUTION

  Altitude APs configured with a static Altitude Controller Search List can only connect to Summit WM Controllers in the list. Improperly configured Altitude APs cannot connect to a non-existent Summit WM Controller address, and therefore cannot receive a corrected configuration.

- **Step 3 - Use Dynamic Host Configuration Protocol (DHCP) Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.**

  To use the DHCP and unicast SLP discovery method, you must ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The Altitude APs use this method to discover the Summit WM Controller.

  This solution takes advantage of two services that are present on most networks:

  - **DHCP (Dynamic Host Configuration Protocol)** - The standard is a means of providing IP addresses dynamically to devices on a network.

- **SLP (Service Location Protocol)** - A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

The Summit WM Controller contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Extreme. The Summit WM Controller contains a DA (SLPD).

The Altitude AP queries DHCP servers for Option 78 in order to locate any DAs. The Altitude APs SLP User Agent then queries the DAs for a list of Extreme Networks SAs.

Option 78 must be set for the subnets connected to the ports of the Summit WM Controller and the subnets connected to the Altitude APs. These subnets must contain an identical list of DA IP addresses.

- **Step 4 - Use a Domain Name Server (DNS) lookup for the host name ext-summitwm-connect-1.domain-name.**

  If no DA is found, or if it has no Extreme Networks SAs registered, the Altitude AP attempts to locate a Summit WM Controller via DNS.

  If you use this method for discovery, place an A record in the DNS server for ext-summitwm-connect-1.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

- **Step 5 - Use a multicast SLP request to find SLP SAs.**

  If all of the preceding methods fail to locate a Summit WM Controller, the Altitude AP sends a multicast SLP request, looking for any SLP Service Agents providing the Extreme Networks service.

Registration after discovery

Any of the discovery steps 2 through 5 can inform the Altitude AP of a list of multiple IP addresses to which the Altitude AP may attempt to connect. Once the Altitude AP has discovered these addresses, it sends out connection requests to each of them. These requests are sent simultaneously. The Altitude AP will attempt to register only with the first which responds to its request.

When the Altitude AP obtains the IP address of the Summit WM Controller, it connects and registers, sending its serial number identifier to the Summit WM Controller, and receiving from the Summit WM Controller a port IP address and binding key.

Once the Altitude AP is registered with a Summit WM Controller, the Altitude AP must be configured. After the Altitude AP is registered and configured, it can be assigned to a WM Access Domain Service (WM-AD) to handle wireless traffic.

Default Altitude AP configuration

Default Altitude AP configuration simplifies the registration after discovery process. Default Altitude AP configuration acts as a configuration template that can be automatically assigned to new registering Altitude APs. The default Altitude AP configuration allows you to specify common sets of radio configuration parameters and WM-AD assignments for Altitude APs. For more information, see "Configuring the default Altitude AP settings" on page 125.

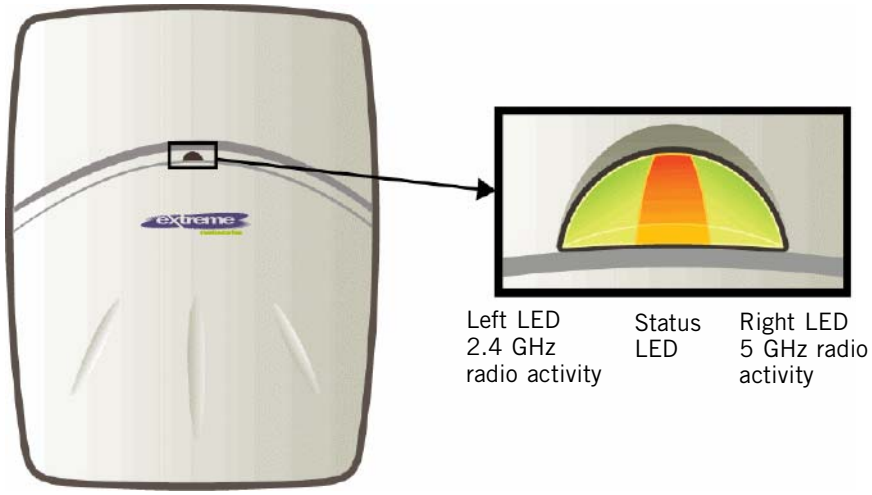
Understanding the Altitude AP LED status

When the Altitude AP is powered on and boots, you can follow its progress through the registration process by observing the LED sequence as described in the following sections.

Altitude AP LED status

The following figure depicts the location of the three LEDs on the Altitude AP.

Figure 7: Altitude AP LEDs



WARNING!

Never disconnect an Altitude AP from its power supply during a firmware upgrade.
Disconnecting an Altitude AP from its power supply during a firmware upgrade may cause firmware corruption rendering the AP unusable.

LEDs color codes

The AP LEDs indicate "normal-operation", "warning/special", or "failed" state of the Altitude AP in the following color codes:

- Green - Indicates the normal-operation state.
- Orange/Amber - Indicates the warning, or special state such as WDS.
- Red - Indicates the error state.
- Blinking - Indicates that the state, such as initialization, or discovery is in progress.
- Steady - Indicates that the state is stable/completed. For example, initialization finished, or discovery completed.

Center LED

The Center LED indicates the general status of the Altitude AP:

Table 5: Center LED and Altitude AP's status

Center LED	Altitude AP's status
Blinking Green	Initialization and discovery in progress via Ethernet link
Blinking Orange/Amber	Initialization and discovery in progress via WDS link
Blinking Red	Error during initialization/discovery process
Solid Red	Irrecoverable error
Solid Green	Discovery finished via Ethernet link
Solid Orange/Amber	Discovery finished via WDS link

Left LED

The Left LED indicates the high-level state of the Altitude AP during the initialization and discovery process:

Table 6: Left LED and Altitude AP's high-level state

Left LED	Altitude AP's high-level state
Off	Initialization
Blinking Green	Network Discovery
Solid Green	Connecting with the Summit WM Controller

Left and Right LEDs

The Right LED indicates the detailed state during the initialization and discovery processes:

Table 7: Left and Right LEDs and Altitude AP's detailed state

Left LED	Right LED	Altitude AP's detailed state
Off	Off	Initialization: Power-on self-test (POST)
	Blinking Green	Initialization: Random delay
	Solid Green	Initialization: Vulnerable period
Blinking Green	Off	Network Discovery: 802.1X authentication
	Blinking Green	Network Discovery: Attempting to obtain IP address via DHCP
	Solid Green	Network Discovery: Discovered Summit WM Controller
Solid Green	Off	Connecting to Summit WM Controller: Attempting to register with the Summit WM Controller
	Blinking Green	Connecting to Summit WM Controller: Upgrading to higher version
	Solid Green	Connecting to Summit WM Controller: Configuring itself

Composite view of the three LEDs

The Center, Left and the Right LEDs work in conjunction to indicate the general, high-level state and the detailed state respectively.

The following table provides a composite view of the three LED lights of the Altitude AP's state:

Table 8: Composite view of three LED lights

Left LED	Right LED	Center LED	Altitude AP's Detailed state
Off	Off	Blinking Green	Initialization: Power-on self-test (POST)
	Blinking Green	Blinking Green	Initialization: Random delay
		Blinking Red	Initialization: Neither Ethernet nor WDS link
	Solid Green	Blinking Green	Initialization: Vulnerable period
		Blinking Red	Reset to factory defaults
	Solid Green	Blinking Orange	WDS scanning
Blinking Green	Off	Blinking Green / Orange	Network discovery: 802.1x authentication
		Blinking Red	Failed 802.1x authentication
	Blinking Green	Blinking Green / Orange	Network discovery: DHCP
		Blinking Red	Default IP address
	Solid Green	Blinking Green / Orange	Network discovery: WM discovery / connect
		Blinking Red	Discovery failed
Solid Green	Off	Blinking Green / Orange	Connecting with Summit WM Controller: Registration
		Blinking Red	Registration failed
	Blinking Green	Blinking Green / Orange	Connecting with Summit WM Controller: Image upgrade
		Blinking Red	Image upgrade failed
	Solid Green	Blinking Green / Orange	Connecting with Summit WM Controller: Configuration
		Blinking Red	Configuration failed
	Blinking Green	Solid Green / Orange	AP operating normally: Forced image upgrade
		Blinking Red	Image upgrade failed

NOTE

The Left and Right LEDs turn on after the center LED. This allows you to distinguish easily between the Center LED and the Left/Right LEDs.

NOTE

If the Center LED begins blinking RED, it indicates that the Altitude AP's state has failed.

NOTE

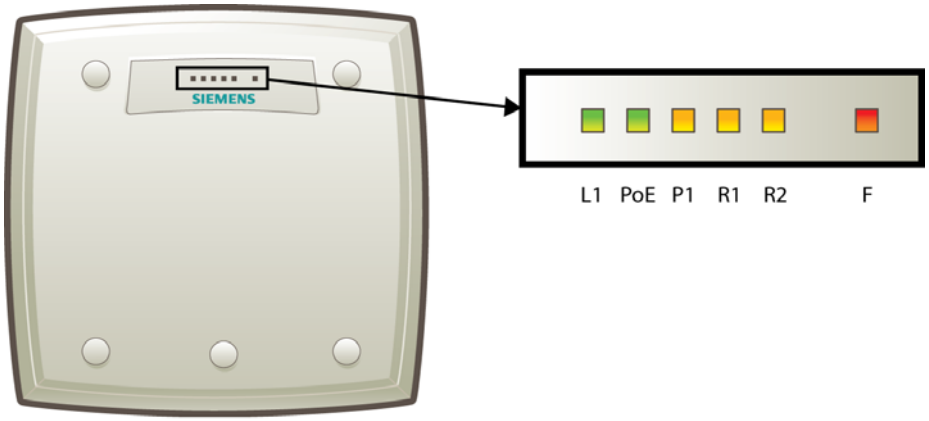
Random delays do not occur during normal reboot. A random delay only occurs after vulnerable period power-down.

The Altitude AP can be reset to its factory default settings. For more information, see the Summit WM Maintenance Guide.

Outdoor AP LED status

The following figure depicts the location of the LEDs on the Outdoor AP.

Figure 8: Outdoor AP LEDs



NOTE

Although the Outdoor AP has six LEDS, only R1, R2 and F LEDs are used in the current release. The remaining LEDs are disabled.

The Center, Left, and the Right LEDs work in conjunction to indicate the general, high-level and detailed state respectively.

The following table provides a composite view of the three LED lights of the Outdoor AP's state:

Table 9: Outdoor AP LED status

R1 LED	R2 LED	F LED	Outdoor AP's detailed status
Off	Off	Blinking Red	Initialization: Power-on-self test (POST)
	Blinking Green	Blinking Red	Initialization: Random delay
	Solid Green	Blinking Red	Initialization: Vulnerable Period
		Solid Red	Reset to factory defaults
	Solid Green	Blink Red	WDS scanning
Blinking Green/ Yellow	Off	Blinking Red	Network discovery: 802.1X authentication
		Solid Red	Failed 802.1X authentication
	Blinking Green/ Yellow	Blinking Red	Network discovery: DHCP
		Solid Red	Default IP address
	Solid Green/ Yellow	Blinking Red	Network discovery: WM discovery/connect
		Solid Red	Discovery failed

Table 9: Outdoor AP LED status (Continued)

R1 LED	R2 LED	F LED	Outdoor AP's detailed status
Solid Green	Off	Blinking Red	Connecting with WM: Registration
		Solid Red	Registration failed
	Blinking Green/ Yellow	Blinking Red	Connecting with WM: Image upgrade
		Solid Red	Image upgrade failed
	Solid Green/ Yellow	Blinking Red	Connecting with WM: Configuration
		Solid Red	Configuration failed
	Blinking Green/ Yellow	Off	AP operating and running normally: Forced image upgrade
		Solid Red	Image upgrade failed

NOTE

After discovery is finished, the Left and Right LEDs will be Green for Ethernet uplink, and Yellow for WDS uplink.

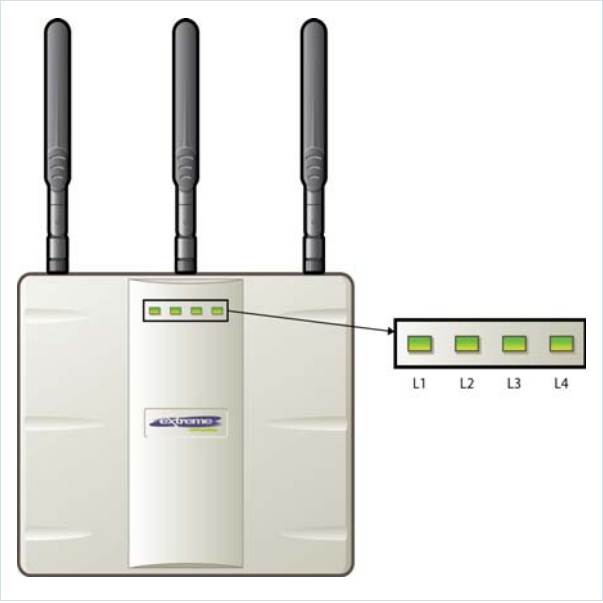
NOTE

If the fatal AP error occurs, the Status LED will be solid Red.

Altitude 802.11n AP LED status

Figure 9 depicts the location of the LEDs on the Altitude 802.11n AP.

Figure 9: Altitude 802.11n AP LEDs



The LEDs, L1, L3 and L4 work in conjunction to indicate the general, high-level, and detailed state respectively.

After initialization and discovery is completed and the 802.11n AP is connected to the Summit WM Controller, the LEDs L3 and L4 indicate the state of the corresponding radio - L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

The LED L2 indicates the status of the Ethernet port.

LEDs color codes

The 802.11n AP LEDs indicate "normal-operation", "warning/special", or "failed" state of the Altitude AP in the following color codes:

- Green - Indicates the normal-operation state.
- Orange/Amber - Indicates the warning, or special state such as WDS.
- Red - Indicates the error state.
- Blinking - Indicates that the state, such as initialization, or discovery is in progress.
- Steady - Indicates that the state is stable/completed. For example, initialization finished, or discovery completed.

LED L1

The LED L1 indicates the general state of the 802.11n AP:

Table 10: LED L1 and Altitude AP's status

L1	Altitude 802.11n AP's general state
Blink Green	Initialization and discovery in progress via Ethernet
Blink Amber	Initialization and discovery in progress via WDS
Blink Red	Error during initialization and discovery
Solid Green	Discovery finished via Ethernet
Solid Amber	Discovery finished via WDS

LEDs L3 and L4

The LEDs L3 and L4 indicate the detailed state of the Altitude AP. The LED1, and LEDs L3 and L4 work in conjunction to indicate the general and detailed state of the 802.11n AP.

Table 11 provides a composite view of the three LEDs and the corresponding state of the 802.11n AP:

Table 11: LEDs L3, L4 and L1, and Wireless 802.11n AP's detailed state

L3	L4	L1	Altitude 802.11n AP's detailed state
Off	Off	Blink Green	Initialization: Power-on self test (POST)
	Blink Green	Blink Green	
		Blink Red	
	Solid Green	Blink Green	
		Blink Red	
	Solid Green	Blink Amber	

Table 11: LEDs L3, L4 and L1, and Wireless 802.11n AP's detailed state (Continued)

L3	L4	L1	Altitude 802.11n AP's detailed state
Blink Green	Off	Blink Green / Amber	Network discovery: 802.1x authentication
		Blink Red	Failed 802.1x authentication
	Blink Green	Blink Green / Amber	Network discovery: DHCP
		Blink Red	Default IP address
	Solid Green	Blink Green / Amber	Network discovery: WM discovery / connect
		Blink Red	Discovery failed
Solid Green	Off	Blink Green / Amber	Connecting to WM: Registration
		Blink Red	Registration failed
	Blink Green	Blink Green / Amber	Connecting to WM: Image upgrade
		Blink Red	Image upgrade failed
	Solid Green	Blink Green / Amber	Connecting to WM: Configuration
		Blink Red	Configuration failed
	Blink Green	Solid Green / Amber	AP operating normally: Forced image upgrade
		Blink Red	Image upgrade failed

After initialization and discovery is completed and the 802.11n AP is connected to the Summit WM Controller, the LEDs L3 and L4 indicate the state of the corresponding radio - L3 for Radio 5 GHz, and L4 for Radio 2.4 GHz.

Figure 12 provides a view of the LEDs L3 and L4 and the corresponding radio state after the discovery is completed.

Table 12: LEDs L3 and L4, and corresponding radio state

L3/L4	Radio status
Off	Radio off
Solid Blue	Radio in HT mode
Solid Green	Radio in legacy mode

LED L2

The LED L2 indicates the status of the Ethernet port:

Table 13: LED L2 and Ethernet port's status

L2	Ethernet port's status
Off	No Ethernet connection: WDS is enabled
Solid Blue	1 Gb Ethernet connection
Solid Green	100 Mb connection
Solid Amber	10 Mb connection

NOTE

A 10 Mb Ethernet connection is considered a warning state since it is not sufficient to sustain a single radio in the legacy 11g or 11a modes.

Configuring the Altitude APs for the first time

Before the Altitude AP is configured for the first time, you must first confirm that the following has already occurred:

- The Summit WM Controller has been set up. For more information, see Chapter 2, "Configuring the Summit WM Controller."
- The Controller, Access Points, and WM software has been configured. For more information, see Chapter 2, "Configuring the Summit WM Controller."
- The Altitude APs have been installed.

NOTE

- If you are installing the Altitude AP, see the Altitude 350-2i/350-2d AP Installation Guide.
- If you are installing the Altitude 802.11n AP, see the Altitude 802.11n AP Installation Guide.
- If you are installing the Outdoor AP, see the specific Siemens brand (SEN or A&D) Outdoor AP Installation Guide.

Once the above processes are complete, you can then continue with the Altitude AP initial configuration. The Altitude AP initial configuration involves two steps:

- **Step One** - Define parameters for the discovery process. For more information, see "Defining properties for the discovery process" on page 80.
- **Step Two** - Connect the Altitude AP to a power source to initiate the discovery and registration process. For more information, see "Connecting the Altitude AP to a power source and initiating the discovery and registration process" on page 82.

Adding a Altitude AP manually option

An alternative to the automatic discovery and registration process of the Altitude AP is to manually add and register a Altitude AP to the Summit WM Controller. For more information, see "Adding and registering an Altitude AP manually" on page 83.

Defining properties for the discovery process

Before an Altitude AP is configured, you must define properties for the discovery process. The discovery process is the process by which the Altitude APs determine the IP address of the Summit WM Controller.

The properties that need to be defined are:

- Security mode
- Discovery timers

Security mode

Security mode is a Summit WM Controller property. It defines how the controller behaves when registering new, unknown devices. During the registration process, the Summit WM Controller's approval of the Altitude AP's serial number depends on the security mode that has been set:

- **Allow all Altitude APs to connect**
  - If the Summit WM Controller does not recognize the registering serial number, a new registration record is automatically created for the AP (if within software license limit). The AP receives a default configuration. The default configuration can be the default template assignment.
  - If the Summit WM Controller recognizes the serial number, it indicates that the registering device is pre-registered with the controller. The controller uses the existing registration record to authenticate the AP and the existing configuration record to configure the AP.
- **Allow only approved Altitude APs to connect (this is also known as secure mode)**
  - If Summit WM Controller does not recognize the AP, the AP's registration record is created in pending state (if within software license limits). The administrator is required to manually approve a pending AP for it to provide active service. The pending AP receives minimum configuration, which only allows it to maintain an active link with the controller for future state change. The AP's radios are not configured or enabled. Pending APs are not eligible for configuration operations (WM-AD Assignment, default template, Radio parameters) until approved.
  - If the Summit WM Controller recognizes the serial number, the controller uses the existing registration record to authenticate the AP. Following successful authentication, the AP is configured according to its stored configuration record.

NOTE

*During the initial setup of the network, it is recommended to select the **Allow all Altitude APs to connect** option. This option is the most efficient way to get a large number of Altitude APs registered with the Summit WM Controller.*

*Once the initial setup is complete, it is recommended that the security mode is reset to the **Allow only approved Altitude APs to connect** option. This option ensures that no unapproved Altitude APs are allowed to connect. For more information, see "Configuring Altitude AP settings" on page 84.*

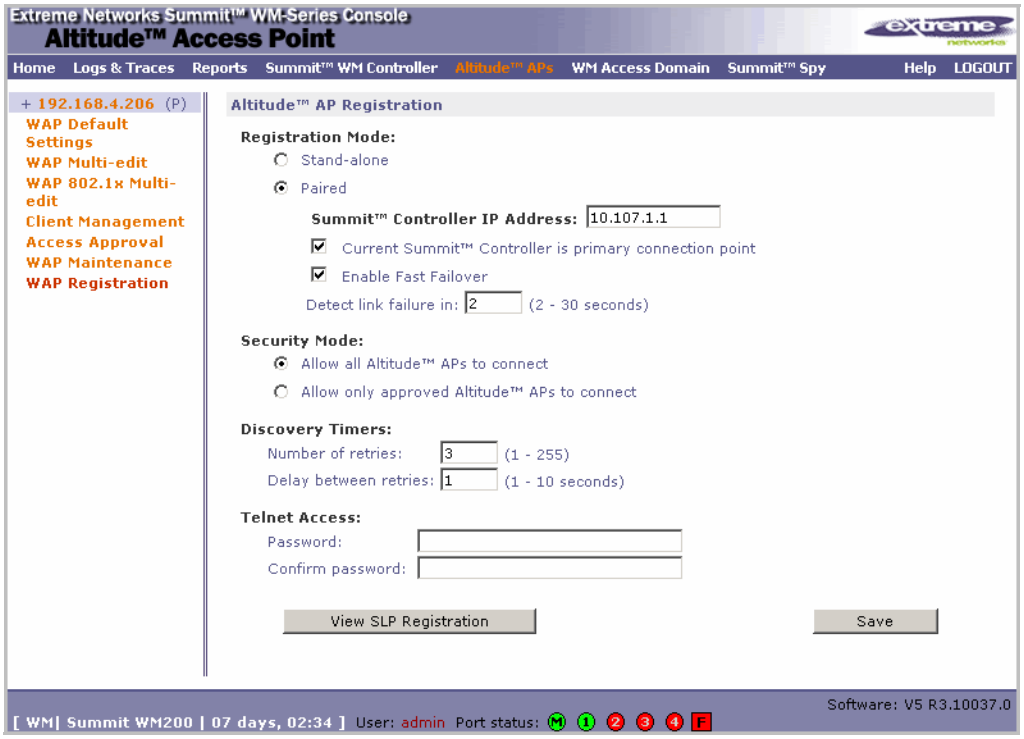
Discovery timers

The discovery timer parameters dictate the number of retry attempts and the time delay between each attempt.

To define the discovery process parameters:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **WAP Registration**. The **WAP Registration** page is displayed.



3 In the **Security Mode** section, select one of the following:

- **Allow all Altitude APs to connect**
- **Allow only approved Altitude APs to connect**

The **Allow all Altitude APs to connect** option is selected by default. For more information, see "Security mode" on page 81.

4 In the **Discovery Timers** section, type the discovery timer values in the following boxes:

- **Number of retries**
- **Delay between retries**

The number of retries is limited to 255 in a five minutes discovery period. The default number of retries is 3, and the default delay between retries is 1 second.

5 To save your changes, click **Save**.

Once the discovery parameters are defined, you can connect the Altitude AP to a power source.

Connecting the Altitude AP to a power source and initiating the discovery and registration process

When an Altitude AP is powered on, it automatically begins the discovery and registration process with the Summit WM Controller.

Altitude AP

The Altitude AP can be connected and powered in the following ways:

- Power over Ethernet (802.3af):
  - PoE enabled switch port
  - PoE Injector
- Power by AC adaptor

Outdoor AP

The Outdoor AP can be connected and powered in the following ways:

- Power over Ethernet
  - PoE enabled switch port
- Power by 48VDC (Direct Current)
- 110-230 VAC (Alternating Current)

For more information, see the *Outdoor AP Installation Guide.*

Altitude 802.11n AP

The Altitude 802.11n can be connected and powered in the following ways:

- Power over Ethernet
  - PoE enabled switch port
  - PoE Injector

NOTE

You should use a 1GB PoE injector to ensure optimum performance of the Altitude 802.11n AP.

- Power by AC adaptor

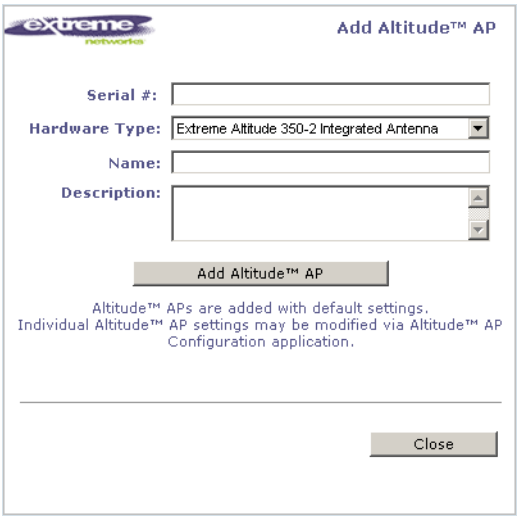
Adding and registering an Altitude AP manually

An alternative to the automatic discovery and registration process of the Altitude AP is to manually add and register an Altitude AP to the Summit WM Controller. The Altitude AP is added with default settings. For more information, see "Configuring Altitude AP settings" on page 84.

To add and register an Altitude AP manually:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 Click **Add Altitude AP**. The **Add Altitude AP** page is displayed.



3 In the **Serial #** box, type the unique identifier.

4 In the **Hardware Type** drop-down list, click the hardware type of the Altitude AP.

5 In the **Name** box, type a unique name for the Altitude AP.

6 In the **Role** drop-down list, click the Altitude AP's role - Access Point.

7 In the **Description** box, type descriptive comments for the Altitude AP.

8 Click **Add Altitude AP**. The Altitude AP is added and registered.

When an Altitude AP is added manually, it is added to the controller database only and does not get assigned.

9 Click **Close**.

Configuring Altitude AP settings

Altitude APs are added with default settings, which you can adjust and configure according to your network requirements. In addition, you can modify the properties and the settings for each radio on the Altitude AP.

You can also locate and select Altitude APs in specific registration states to modify their settings. For example, this feature is useful when approving pending Altitude APs when there are a large number of other Altitude APs that are already registered. On the **Access Approval** page, click **Pending** to select all pending Altitude APs, then click **Approve** to approve all selected Altitude APs.

Configuring Altitude AP settings can include the following processes:

- Modifying an Altitude AP's status
- Modifying an Altitude AP's properties
- Modifying Altitude AP radio properties
- Setting up the Altitude AP using static configuration

- Setting up 802.1X authentication for an Altitude AP

When configuring Altitude APs, you can choose to configure individual Altitude APs or simultaneously configure a group of Altitude APs. For more information, see "Configuring Altitude APs simultaneously" on page 135.

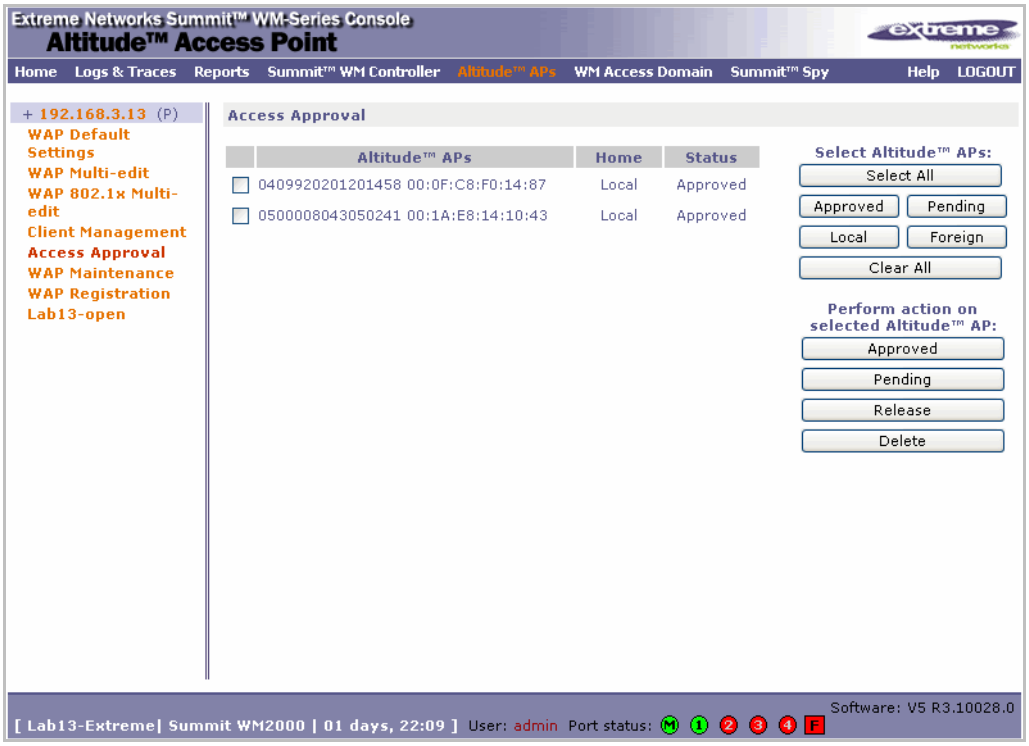
Modifying an Altitude AP's status

If during the discovery process, the Summit WM Controller security mode was **Allow only approved Altitude APs to connect**, then the status of the Altitude AP is Pending. You must modify the security mode to **Allow all Altitude APs to connect**. For more information, see "Security mode" on page 81.

To modify an Altitude AP's registration status:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **Access Approval**. The **Access Approval** page is displayed, along with the registered Altitude APs and their status.



3 To select the Altitude APs for status change, do one of the following:

- For a specific Altitude AP, select the corresponding checkbox.
- For Altitude APs by category, click one of the **Select Altitude APs** options.

NOTE

*You must consider all the three AP variants - Altitude AP, Outdoor AP, and Altitude 802.11n AP - as **Local**.*

To clear your Altitude AP selections, click **Clear All**.

4 Click the appropriate **Perform action on selected Altitude APs** option:

- **Approved** - Change an Altitude AP's status from Pending to Approved, if the **WAP Registration** page was set to register only approved Altitude APs.
- **Pending** - AP is removed from the Active list, and is forced into discovery.
- **Release** - Release foreign Altitude APs after recovery from a failover. Releasing an AP corresponds to the Availability functionality. For more information, see Chapter 6, "Availability and session availability."
- **Delete** - Releases the Altitude AP from the Summit WM Controller and deletes the Altitude AP's entry in the Summit WM Controller's management database.

Modifying an Altitude AP's properties

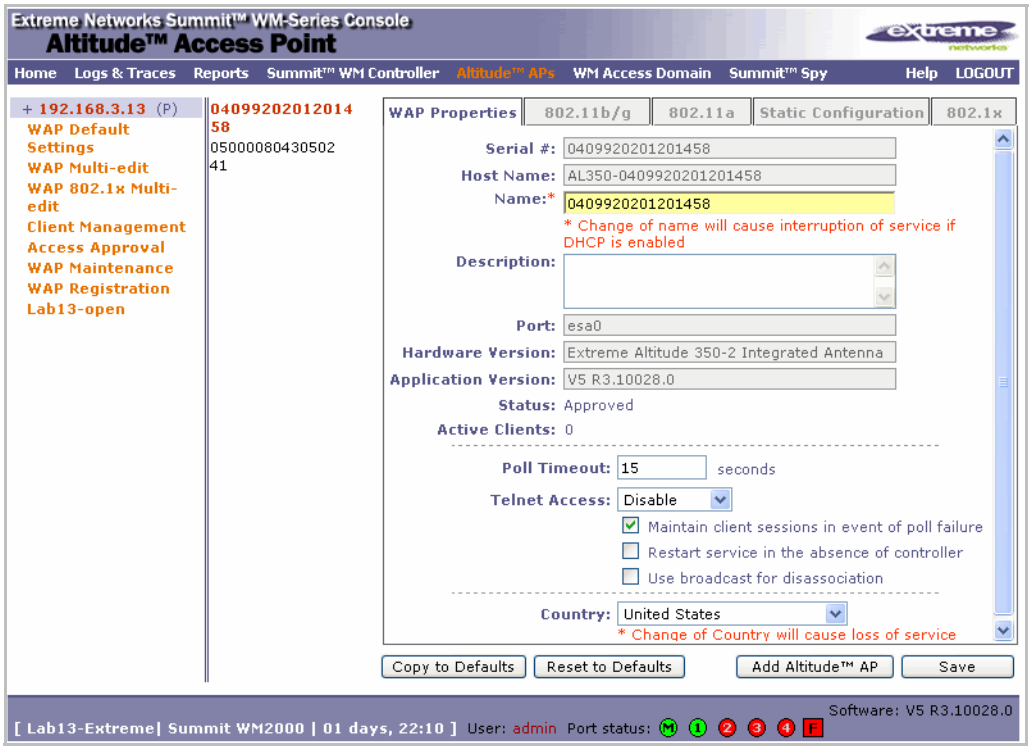
Once an Altitude AP has successfully registered, you can then modify its properties. Modifying an AP's properties can include modifying properties on the following tabs:

- AP properties
- 802.11b/g/n
- 802.11a/n
- Static Configuration
- 802.1X

To modify an Altitude AP's properties:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to modify. The **WAP Properties** tab displays Altitude AP information.



3 Modify the Altitude AP's information:

- **Name** - Type a unique name for the Altitude AP that identifies the AP. The default value is the Altitude AP's serial number.
- **Description** - Type comments for the Altitude AP.
- **WAP Environment** - Click the Altitude AP's environment - **Indoor** or **Outdoor**.

NOTE

*The **WAP Environment** drop-down is displayed on the **WAP Properties** tab only if the selected Altitude AP is the Outdoor AP.*
*Since the Outdoor AP can be deployed in both indoor and outdoor environments, the **WAP Properties** page enables you to specify the environment.*

- **Poll Timeout** - Type the timeout value, in seconds, for the Altitude AP to re-establish the link with the Summit WM Controller if it (Altitude AP) does not get an answer to its polling. The default value is 15 seconds.

NOTE

If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on WAP Properties screen. For more information, see "Session availability" on page 237.

- **Telnet Access** - Click to enable or disable Telnet Access to the Altitude AP.
- **Maintain client session in event of poll failure** - Select this option (if using a bridged at AP WM-AD) if the AP should remain active if a link loss with the controller occurs.This option is enabled by default.
- **Restart service in the absence of controller** - Select this option (if using a bridged at AP WM-AD) to ensure the Altitude APs' radios continue providing service if the Altitude AP's connection to the Summit WM Controller is lost. If this option is enabled, it allows the Altitude AP to start a bridged at AP WM-AD even in the absence of a Summit WM Controller
- **Use broadcast for disassociation** - Select if you want the Altitude AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Altitude AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).
  - If a BSSID is deactivated or removed on the Altitude AP.

  This option is disabled by default.
- **Country** - Click the country of operation. This option is only available with some licenses.

The following on the **WAP Properties** tab are view only:

- **Serial #** - Displays a unique identifier that is assigned during the manufacturing process.
- **Port** - Displays the Ethernet port of the Summit WM Controller the Altitude AP is connected to.
- **Hardware Version** - Displays the current version of the Altitude AP hardware.

NOTE

Any Wireless AP model number in the Hardware Version box that ends with -1 represents a Wireless AP that contains the new Siemens radio card. For example, the HiPath Wireless AP2650-1 Internal.

- **Application Version** - Displays the current version of the Altitude AP software.
- **Status**:
  - **Approved** - Indicates that the Altitude AP has received its binding key from the Summit WM Controller after the discovery process.
  - **Pending** - Indicates that the Altitude AP has not yet successfully been approved for access with the secure controller.

  You can modify the status of a Altitude AP on the **Access Approval** page. For more information, see "Modifying an Altitude AP's status" on page 85
- **Active Clients** - Displays the number of wireless devices currently active on the Altitude AP.

4 To save your changes, click **Save**.

Modifying Altitude AP radio properties

Most properties of the Altitude AP radios can be modified without requiring a reboot of the Altitude AP. However, if the modification of a Altitude AP property does trigger a reboot, the Altitude AP property is identified with a red asterisk in the Summit WM GUI.

NOTE

Modifying Altitude AP radio properties can vary significantly depending on the model of the Altitude AP your are configuring:
- For specific information on modifying an Altitude 802.11n AP, see "Modifying Altitude 802.11n AP 450/451 radio properties" on page 90.
- For specific information on modifying an Altitude AP 350-2i/350-2d or Outdoor AP, see "Modifying Altitude AP 350-2i/350-2d radio properties" on page 106.

Dynamic Radio Management (DRM)

When you modify an Altitude AP's radio properties, the Dynamic Radio Management (DRM) functionality of the Summit WM Controller is used to help establish the optimum radio configuration for your Altitude APs. DRM is enabled by default. The Summit WM Controller's DRM:

- Adjusts transmit power levels to balance coverage between Altitude APs assigned to the same RF domain and operating on the same channel.
- Scans and coordinates with other Altitude APs to select an optimal operating channel.

The DRM feature consists of three functions:

- **Auto Channel Selection (ACS)** - ACS provides an easy way to optimize channel arrangement based on the current situation in the field. ACS provides an optimal solution only if it is triggered on all Altitude APs in a deployment. Triggering ACS on a single Altitude AP or on a subset of Altitude APs provides a useful but suboptimal solution. Also, ACS only relies on the information observed at the time it is triggered. Once an Altitude AP has selected a channel, it will remain operating on that channel until the user changes the channel or triggers ACS.

  ACS can be triggered by one of the following events:

  - A new Altitude AP registers with the Summit WM Controller and the **AP Default Settings** channel is **Auto**.
  - A user selects **Auto** from the **Request New Channel** drop-down list on the Altitude AP's radio configuration tabs.
  - A user selects **Auto** from the **Channel** drop-down list on the **AP Multi-edit** page.
  - If Dynamic Channel Selection (DCS) is enabled in active mode and a DCS threshold is exceeded.
  - An Altitude AP detects radar on its current operating channel and it employs ACS to select a new channel.
  - **Channel Plan** - If ACS is enabled, you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.

    Depending on the radio used, when defining a channel plan you can either create your customized channel plan by selecting individual channels or you can select a default 3 or 4 channel plan.

    You can use the channel plan to avoid transmission overlap on 40 MHz channels of the Altitude 802.11n APs. To avoid channel overlap between Altitude 802.11n APs that operate on 40 MHz channels, configure the channel plan for the 5 GHz radio band as follows: 36, 44, 149, and 157 or 40, 48, 153, and 161. This solution limits the available channels to half of the available channels.

    If using half of the available channels is not an option for your environment, do not configure a channel plan. Instead, allow ACS to select from all available channels. This alternate solution may contribute to increased congestion on the extension channels.

NOTE

ACS in the 2.4 GHz radio band with 40 MHz channels is not recommended due to severe co-channel interference.

- **Dynamic Channel Selection (DCS)** - DCS allow an Altitude AP to monitor traffic and noise levels on the current channel that the Altitude AP operates on. DCS can operate in two modes:
  - **Monitor** - When DCS is enabled in monitor mode and traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. The DCS monitor alarm is used for evaluating the RF environment of your deployed Altitude APs.
  - **Active** - When DCS is enabled in active mode and traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on. DCS will not trigger channel changes on neighboring Altitude APs.

  NOTE

  If DCS is enabled, DCS statistics can be viewed in the Wireless Statistics by Altitude APs display. For more information, see Chapter 10, "Working with reports and displays."

- **Auto Tx Power Control (ATPC)** - ATPC guarantees your LAN a stable RF environment by automatically adapting transmission power signals according to the coverage provided by the Altitude APs. ATPC can be either enabled or disabled. When you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established:
  - If you elect to maintain using the ATPC power setting from an individual Altitude AP edit page, the displayed **Current Tx Power Level** value becomes the new **Max Tx Power** value for that Altitude AP.
  - If you elect to maintain using the ATPC power setting from the **AP Multi-edit** page, for every Altitude AP the **Current Tx Power Level** value in the database is used to set the **Max Tx Power** value.
  - If you elect not to maintain using the ATPC power setting, the current **Max Tx Power** value is applied.

Modifying Altitude 802.11n AP 450/451 radio properties

The Altitude 802.11n AP 450/451 is a 802.11n (draft)-compliant access point. The following section discusses how to modify an Altitude 802.11n AP.

For information on how to modify an Altitude AP 350-2i/350-2d or the Outdoor AP, see "Modifying Altitude AP 350-2i/350-2d radio properties" on page 106.

Channel bonding

Channel bonding improves the effective throughput of the wireless LAN. In contrast to the Altitude AP 35xx which uses radio channel spacings that are only 20MHz wide, the Altitude 802.11n AP can use two channels at the same time to create a 40MHz wide channel. To achieve a 40MHz channel width, the Altitude 802.11n AP employs channel bonding - two 20MHz channels at the same time.

The 40MHz channel width is achieved by bonding the primary channel (20MHz) with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel.

Depending on the radio protocols, channel bonding can be predefined:

- **802.11b/g/n** - Channels can bond up or down as long as the band edge is not exceeded, but some channels have predefined bonding directions.
- **802.11a/n** - Bonding pairs are predefined.

Channel bonding is enabled by selecting the **Channel Width** on the **802.11b/g/n** and **802.11a/n** tabs. When selecting **Channel Width**, the following options are available:

- **20MHz** - Channel bonding is not enabled:
  - 802.11n clients use the primary channel (20 MHz)
  - Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
- **40MHz** - Channel bonding is enabled:
  - 802.11n clients that support the 40MHz frequency can use 40MHz, 20MHz, or the 802.11a/b/g radio protocols.
  - 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11a/b/g radio protocols.
  - Non-802.11n clients, beacons, and multicasts use the 802.11a/b/g radio protocols.
  - If the primary channel allows for both bonding types (up and down), you can click the channel bond type from the **Channel Bonding** drop-down list.
  - If the primary channel allows for one of the bonding types (up or down), the channel bond type is displayed in the **Channel Bonding** drop-down list.
- **Auto** - Channel bonding is automatically enabled or disabled, switching between 20MHz and 40MHz, depending on how busy the extension channel is. If the extension channel is busy above a prescribed threshold percentage, which is defined in the **40MHz Channel Busy Threshold** box, channel bonding is disabled.

Channel selection - primary and extension

The primary channel of the Altitude 802.11n AP is selected from the **Request New Channel** drop-down list. If **auto** is selected, the ACS feature selects the primary channel. Depending on the primary channel that is selected, channel bonding may be allowed: up, down, both, or neither.

Guard interval

The guard intervals ensure that individual transmissions do not interfere with one another. The Altitude 802.11n AP provides a shorter guard interval that increases the channel throughput. When a 40MHz channel is used, you can select the guard interval to improve the channel efficiency. The guard interval is selected from the **Guard Interval** drop-down list. Longer guard periods reduce the channel efficiency.

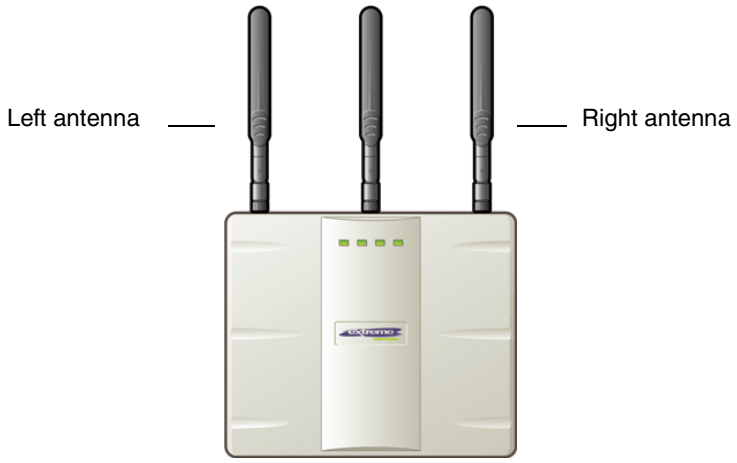
Aggregate MSDU and MPDU

The Altitude 802.11n AP provides aggregate Mac Service Data Unit (MSDU) and aggregate Mac Protocol Data Unit (MPDU) functionality, which combines multiple frames together into one larger frame for a single delivery. This aggregation reduces the overhead of the transmission and results in

increased throughput. The aggregate methods are enabled and defined selected from the **Aggregate MSDUs** and **Aggregate MPDUs** drop-down lists.

Antenna selection

The Altitude 802.11n AP has three antennas: left, middle, and right. The illustration below identifies the left and right antennas.



The Altitude 802.11n AP is configured, by default, to transmit on all three antennas. Depending on your deployment requirements, you can configure the Altitude 802.11n AP to transmit on specific antennas. You can configure the Altitude 802.11n AP to transmit on specific antennas for both radios, including all the available modes:

- radio b/g/n
- radio a/n

When you configure the Altitude 802.11n AP to use specific antennas, the following occurs:

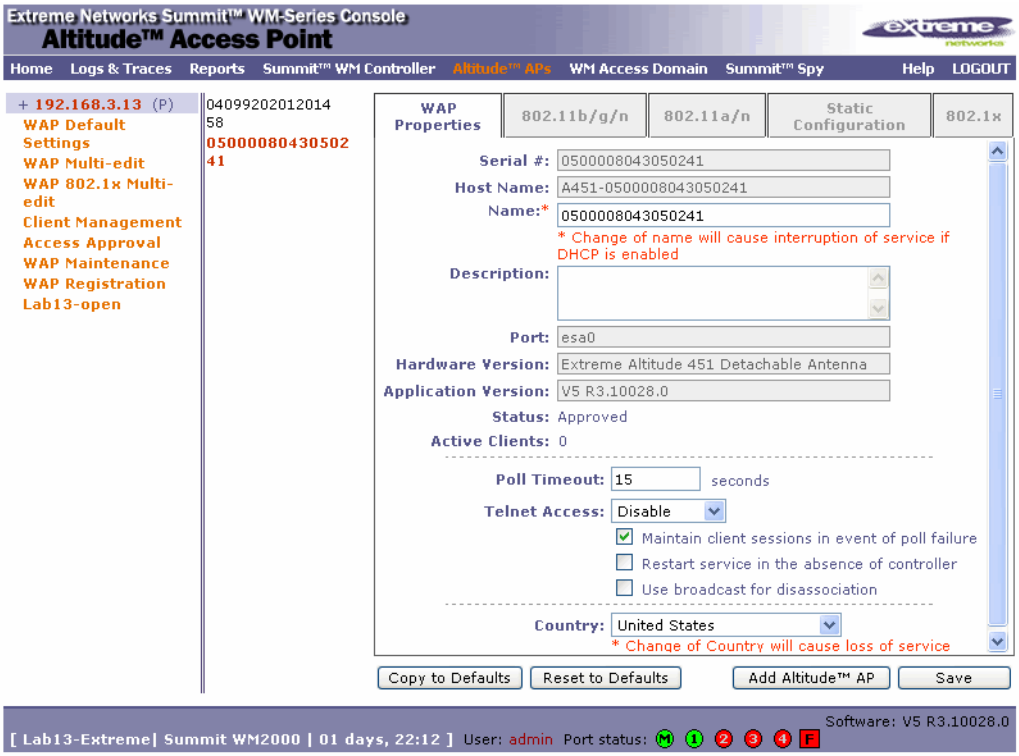
- Transmission power is recalculated - The **Current Tx Power Level** value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the **Current Tx Power Level** value to be reflected in the Altitude 802.11n AP.
- Radio is reset - The radio is reset causing client connections on this radio to be lost.

To modify Altitude 802.11n AP radio properties:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 Click the appropriate Altitude 802.11n AP in the list.

3 If applicable, click the **802.11b/g/n** tab to modify the radio properties:



Each tab displays the radio settings for each radio on the Altitude AP. If the radio has been assigned to a WM-AD, the WM-AD names and MAC addresses are displayed in the **Base Settings** section. The Summit WM Controller can support the following:

- WM200/2000 - Up to 64 WM-ADs
- WM20 - Up to 8 WM-ADs
- WM1000 - Up to 50 WM-ADs
- WM100 - Up to 32 WM-ADs

The Altitude 802.11n AP radios can be assigned to each of the configured WM-ADs in a system. Each radio can be the subject of 8 WM-AD assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

The **BSS Info** section is view only. After WM-AD configuration, the **Basic Service Set (BSS)** section displays the MAC address on the Altitude AP for each WM-AD and the SSIDs of the WM-ADs to which this radio has been assigned.

4 In the **Base Settings** section, do the following:

- **Radio Mode** - Click one of the following radio options:
  - **11b** - Click to select the 802.11b only mode of the 802.11b/g/n radio. If selected, the AP will only use 11b (CCK) rates with all associated clients.
  - **11b/g** - Click to select both the 802.11g mode and the 802.11b mode of the 802.11b/g/n radio. If selected, the AP will use 11b (CCK) and 11g-specific (OFDM) rates with all of the associated clients. The AP will not transmit or receive 11n rates.
  - **11b/g/n** - Click to select 11b/g/n modes of the 802.11b/g/n radio. If selected, the AP will use all available 11b, 11g, and 11n rates.
  - **off** - Click to disable the 802.11b/g/n radio.

NOTE

Depending on the radio options you select, some of the radio settings may not be available for configuration.

- **Channel Width** - Click the channel width for the radio:
  - **20MHz** - Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols.
  - **40MHz** - Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols.
  - **Auto** - Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM Period** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** - Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** - Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** - Type the fragment size threshold, in bytes, above which the packets will be fragmented by the Altitude 802.11n AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

5 In the **Basic Radio Settings** section, do the following:

- **Request New Channel** - Click the wireless channel you want the Wireless 802.11n AP to use to communicate with wireless devices.

  Click **Auto** to request the ACS to search for a new channel for the Wireless 802.11n AP, using a channel selection algorithm. This forces the Wireless 802.11n AP to go through the auto-channel selection process again.

NOTE

ACS in the 2.4 GHz radio band with 40 MHz channels is not recommended due to severe co-channel interference.

  Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information."
- **Channel Bonding** - Click the bonding method, **Up** or **Down**. The primary channel (20MHz) is bonded with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel. Depending on the channel that is selected in the **Request New Channel** drop-down list, you may be prevented from bonding **Up** or **Down** in the **Channel Bonding** drop-down list.
- **Guard Interval** - Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).

- **Max Tx Power** - Click the maximum Tx power level that the range of transmit power can be adjusted: 0 to 23 dBm. It is recommended to use 23 dBm to not limit the potential Tx power level range that can be used.
- **Min Tx Power** - If ATPC is enabled, click the Tx power level that the range of transmit power can be adjusted. It is recommended to use the lowest value available to not limit the potential Tx power level range that can be used.

NOTE

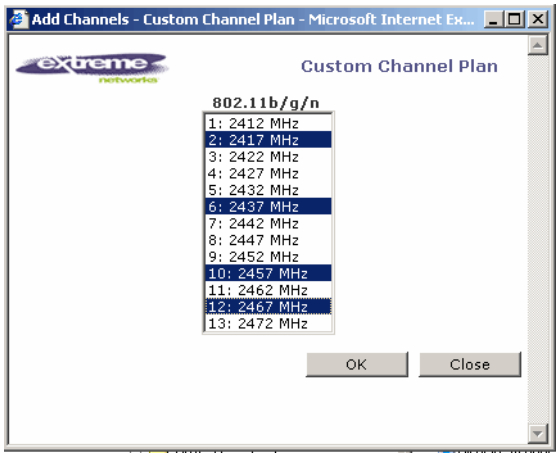
The Minimum Tx Power level is subject to the regulatory compliance requirement for the selected country.

- **Auto Tx Power Ctrl Adjust** - If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use 0 dB during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Current Channel** - This field is view only. It displays the actual channel the ACS has assigned to the Altitude 802.11n AP radio. The **Current Channel** value and the **Last Requested Channel** value may be different because the ACS automatically assigns the best available channel to the Altitude 802.11n AP, ensuring that a Altitude 802.11n AP's radio is always operating on the best available channel.
- **Last Requested Channel** - This field is view only. This field displays the last wireless channel that you had selected for the Altitude AP to communicate with the wireless devices.
- **Auto Tx Power Ctrl (ATPC)** - Select to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.

NOTE

If you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established. If you elect to maintain using the ATPC power setting, the displayed Current Tx Power Level value becomes the new Max Tx Power value for the Altitude AP.

- **Current Tx Power Level** - This field is view only. It displays the actual Tx power level assigned to the Altitude 802.11n AP radio.
- **Channel Plan** - If ACS is enabled, you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference. Click one of the following:
  - **3 Channel Plan** - ACS will scan the following channels: 1, 6, and 11 in the US, and 1, 7, and 13 in Europe.
  - **4 Channel Plan** - ACS will scan the following channels: 1, 4, 7, and 11 in the US, and 1, 5, 9, and 13 in Europe.
  - **Auto** - ACS will scan the default channel plan channels: 1, 6, and 11 in the US, and 1, 5, 9, and 13 in Europe.
  - **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.



- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger **ACS**.
- **Antenna Selection** - Click the antenna, or antenna combination, you want to configure on this radio.

NOTE

When you configure the Wireless 802.11n AP to use specific antennas, the transmission power is recalculated; the Current Tx Power Level value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the Current Tx Power Level value to be reflected in the Summit WM GUI. Also, the radio is reset; the radio is reset causing client connections on this radio to be lost.

6 In the **11b Settings** section, do the following:

- **Preamble** - Click a preamble type for 11b-specific (CCK) rates: **Short** or **Long**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this Altitude 802.11n AP. Click **Long** if compatibility with pre-11b clients is required.

7 In the **11g Settings** section, do the following:

- **Protection Mode** - Click a protection mode: **None** or **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.

- **Protection Type** - Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

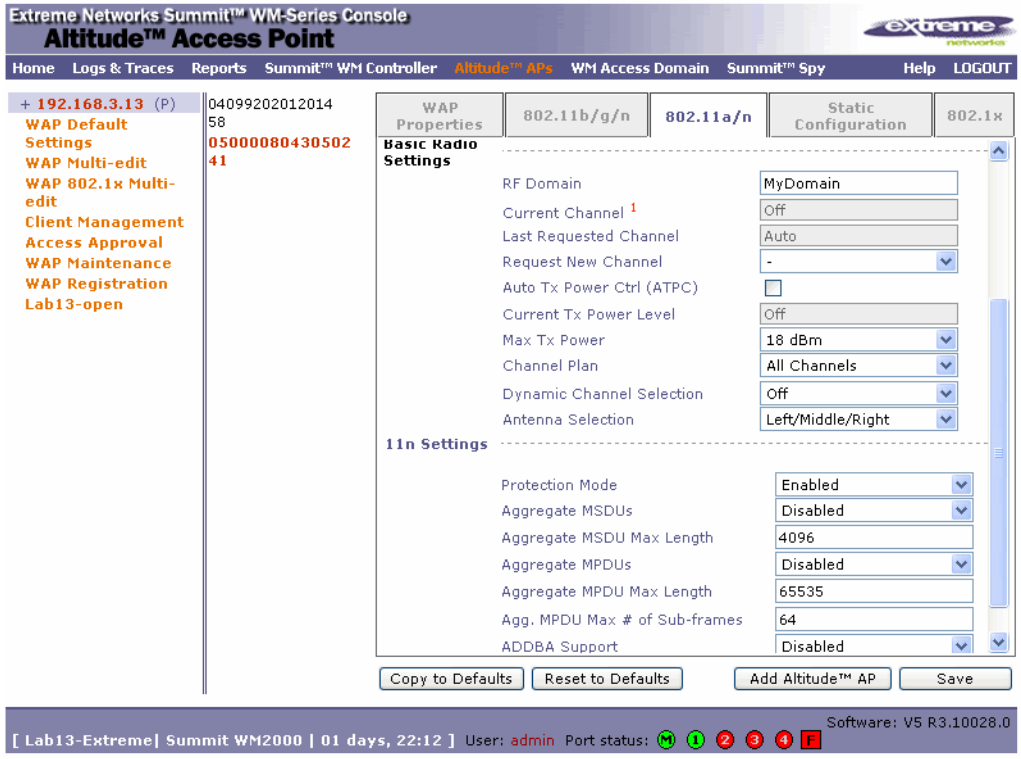
NOTE

*The overall throughput is reduced when **Protection Mode** is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting **Protection Type** to **CTS Only**. Although, the overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended to disable 11g support (11g clients are backward compatible with 11b APs).*
An alternate approach, although a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

8 In the **11n Settings** section, do the following:

- **Protection Mode** - Click a protection mode: **Enabled** or **Disabled**. This protects high throughput transmissions on primary channels from non-11n APs and clients. Click **Disabled** if non-11n APs and clients are not expected. Click **Enabled** if you expect many non-11n APs and clients. The overall throughput is reduced when **Protection Mode** is enabled.
- **40MHz Protection Mode** - Click a protection type, **CTS Only** or **RTS- CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
- **40MHz Prot. Channel Offset** - Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels 1, 5, 9, and 13) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels 1, 6, and 11.
- **40MHz Channel Busy Threshold** - Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
- **Aggregate MSDUs** - Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
- **Aggregate MSDU Max Length** - Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
- **Aggregate MPDUs** - Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput.
- **Aggregate MPDU Max Length** - Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
- **Agg. MPDU Max # of Sub-frames** - Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
- **ADDBA Support** - Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.

9 If applicable, click the **802.11a/n** tab to modify the radio properties:



10 In the **Base Settings** section, do the following:

- **Radio Mode** - Click one of the following radio options:
  - **a** - Click to enable only the 802.11a mode of the 802.11a/n radio.
  - **a/n** - Click to enable both the 802.11a mode and the 802.11n mode of the 802.11a/n radio.
  - **off** - Click to disable the 802.11a/n radio.

NOTE

Depending on the radio options you select, some of the radio settings may not be available for configuration.

- **Channel Width** - Click the channel width for the radio:
  - **20MHz** - Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11a radio protocols.
  - **40MHz** - Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11a radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11a radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11a radio protocols.
  - **Auto** - Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM Period** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** - Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.

- **RTS/CTS Threshold** - Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** - Type the fragment size threshold, in bytes, above which the packets will be fragmented by the Altitude 802.11n AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

11 In the **Basic Radio Settings** section, do the following:

- **Request New Channel** - Click the wireless channel you want the Altitude 802.11n AP to use to communicate with wireless devices.

  Click **Auto** to request the ACS to search for a new channel for the Altitude AP, using a channel selection algorithm. This forces the Altitude 802.11n AP to go through the auto-channel selection process again.

  Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information."
- **Guard Interval** - Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).
- **Max Tx Power** - Click the maximum Tx power level that the range of transmit power can be adjusted: 0 to 24 dBm. It is recommended to use 24 dBm to not limit the potential Tx power level range that can be used.
- **Min Tx Power** - If ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted. It is recommended to use the lowest value available to not limit the potential Tx power level range that can be used.

NOTE

The Minimum Tx Power level is subject to the regulatory compliance requirement for the selected country.

- **Auto Tx Power Ctrl Adjust** - If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use 0 dB during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Current Channel** - This field is view only. It displays the actual channel the ACS has assigned to the Altitude 802.11n AP radio. The **Current Channel** value and the **Request New Channel** value may be different because the ACS automatically assigns the best available channel to the Altitude 802.11n AP, ensuring that a Altitude 802.11n AP's radio is always operating on the best available channel.
- **Last Requested Channel** - This field displays the last wireless channel that you had selected for the Altitude 802.11n AP to communicate with the wireless devices.
- **Auto Tx Power Ctrl (ATPC)** - Select to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.

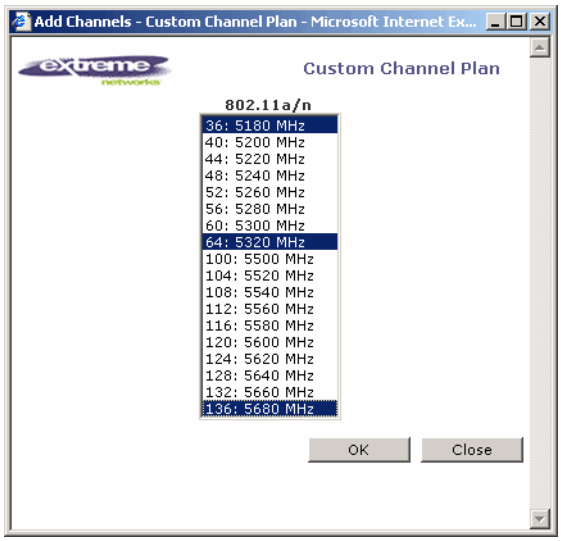
NOTE

If you disable ATPC, you can elect to maintain using the current Tx power setting ATPC had established. If you elect to maintain using the ATPC power setting, the displayed Current Tx Power Level value becomes the new Max Tx Power value for the Altitude AP.

- **Current Tx Power Level** - This field is view only. It displays the actual Tx power level assigned to the Altitude 802.11n AP radio.
- **Channel Plan** - If ACS is enabled, you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference. Click one of the following:
  - **All channels** - ACS will scan all the channels for an operating channel.
  - **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.

NOTE

You can use the channel plan to avoid transmission overlap on 40MHz channels of the Wireless 802.11n APs. For more information, see "Dynamic Radio Management (DRM)" on page 89



- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.

- **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
- **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger **ACS**.

- **Antenna Selection** - Click the antenna, or antenna combination, you want to configure on this radio.

NOTE

When you configure the Wireless 802.11n AP to use specific antennas, the transmission power is recalculated; the Current Tx Power Level value for the radio is automatically adjusted to reflect the recent antenna configuration. It takes approximately 30 seconds for the change to the Current Tx Power Level value to be reflected in the Summit WM GUI. Also, the radio is reset; the radio is reset causing client connections on this radio to be lost.

12 In the **11n Settings** section, do the following:

- **Protection Mode** - Click a protection mode: **Enabled** or **Disabled**. This protects high throughput transmissions on primary channels from non-11n APs and clients. Click **Disabled** if non-11n APs and clients are not expected. Click **Enabled** if you expect many non-11n APs and clients. The overall throughput is reduced when **Protection Mode** is enabled.
- **40MHz Protection Mode** - Click a protection type, **CTS Only** or **RTS- CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.
- **40MHz Prot. Channel Offset** - Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels 1, 5, 9, and 13) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels 1, 6, and 11).
- **40MHz Channel Busy Threshold** - Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
- **Aggregate MSDUs** - Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
- **Aggregate MSDU Max Length** - Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
- **Aggregate MPDUs** - Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput.
- **Aggregate MPDU Max Length** - Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
- **Agg. MPDU Max # of Sub-frames** - Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.
- **ADDBA Support** - Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.

13 To save your changes, click **Save.**

Achieving high throughput with the Wireless 802.11n AP

To achieve link rates of up to 300 Mbps with the Wireless 802.11n AP, configure your system as described in the following section.

NOTE

Maximum throughput cannot be achieved if both 802.11n and legacy client devices are to be supported.

NOTE

Some client devices will choose a 2.4 GHz radio even when a 5 GHz high-speed radio network is available; you may need to force those client devices to use only 5 GHz if you have configured high throughput only on the 5 GHz radio.

To achieve high throughput with the Altitude 802.11n AP:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP** page is displayed.

2 In the **Altitude AP** list, click the Wireless 802.11n AP you want to configure.

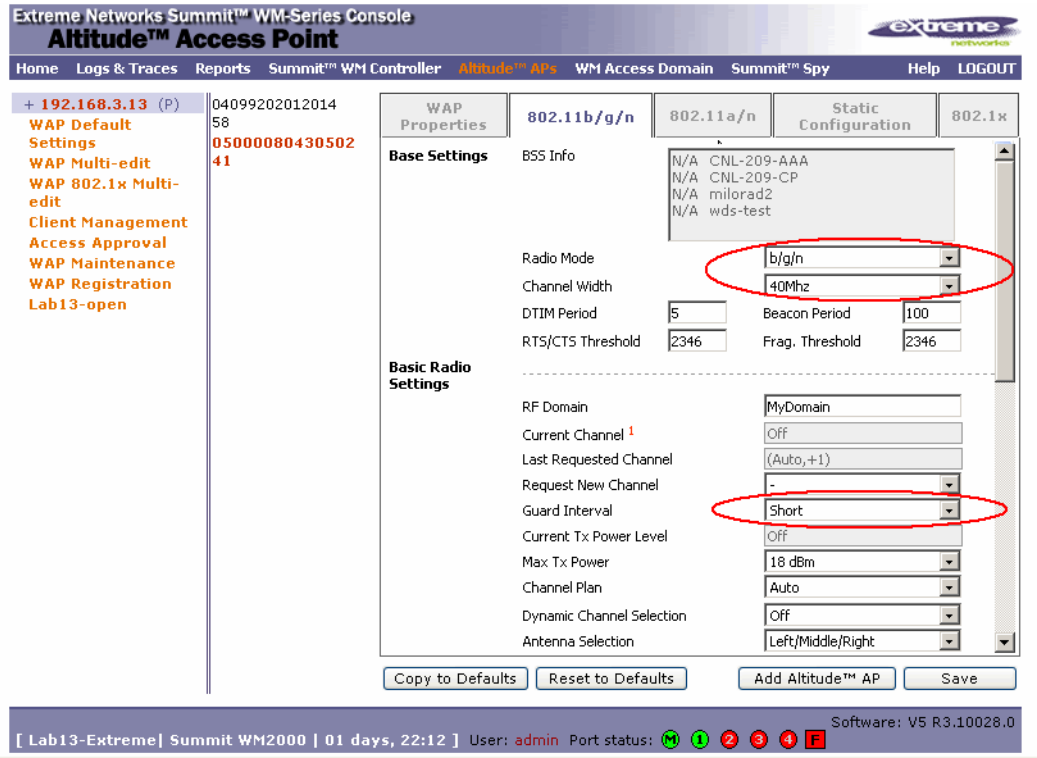
3 Click the **802.11b/g/n** tab, and then do the following:

- In the **Radio Mode** drop-down list, click the **b/g/n** option.
- In the **Channel Width** drop-down list, click **40MHz**.

NOTE

Some client devices do not support 40MHz in b/g/n mode. To accommodate these clients, you must enable a/n mode on the 802.11a/n tab. Otherwise, the client device will connect at only 130Mbps.

- In the **Guard Interval** drop-down list, click **Short**.



- 802.11g protection mode must be disabled:
  - In the 11g Settings section, click **None** in the **Protection Mode** drop-down list.

NOTE

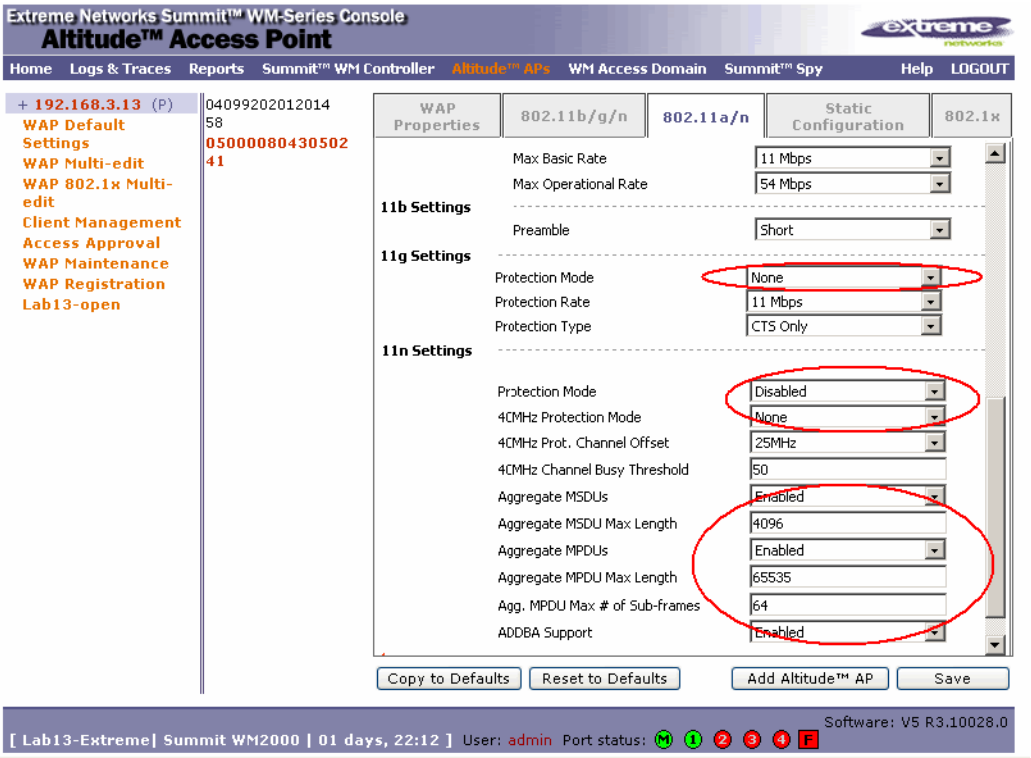
Do not disable 802.11g protection mode if you have 802.11b client devices using this Altitude AP; instead, configure only the 5GHz radio for high throughput (on the 802.11a/n tab) unless it is acceptable to achieve less than maximum 802.11n throughput on the 2.4GHz radio.

- If only 802.11n devices are present, 11n protection and 40Mz protection must be disabled:
  - **Protection Mode** - Click **Disabled**.
  - **40MHz Protection Mode** - Click **None**.

NOTE

Do not disable 802.11n protection mode if you have 802.11b client devices using this Altitude AP; instead, configure only the 5GHz radio for high throughput (on the 802.11a/n tab) unless it is acceptable to achieve less than maximum 802.11n throughput on the 2.4GHz radio.

- **Aggregate MSDUs** - Click **Enabled**.
- **Aggregate MSDU Max Length** - Type **4096.**
- **Aggregate MPDU** - Click **Enabled**.
- **Aggregate MPDU Max Length** - Click **65535.**
- **Agg. MPDU Max # of Sub-frames** - Type **64**.
- **ADDBA Support** - Click **Enabled**.



4 Click the **802.11a/n** tab, and then do the following:

- In the **Radio Mode** drop-down list, click the **a/n** option.
- In the **Channel Width** drop-down list, click **40MHz**.
- In the **Guard Interval** drop-down list, click **Short**.
- If only 802.11n devices are present, 11n protection and 40MHz protection must be disabled:
  - **Protection Mode** - Click **Disabled**.
  - **40MHz Protection Mode** - Click **None**.

NOTE

Do not disable 802.11n protection mode if you have 802.11b client devices using this Altitude AP; instead, configure only the 5GHz radio for high throughput unless it is acceptable to achieve less than maximum 802.11n throughput on the 2.4GHz radio.

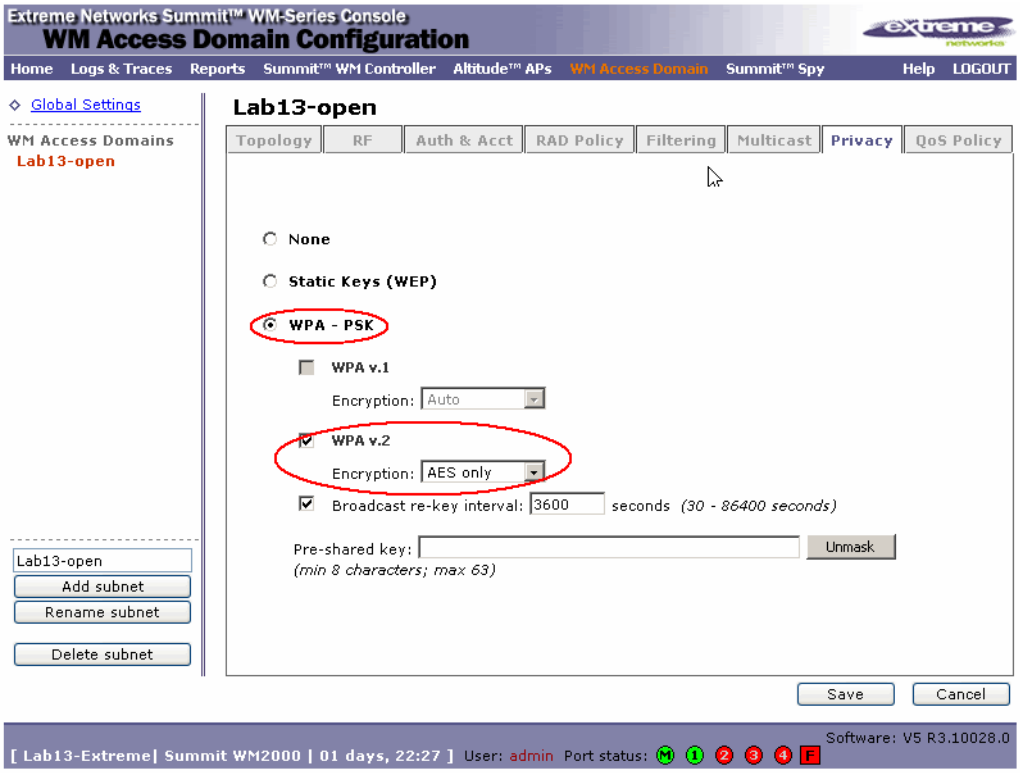
- **Aggregate MSDUs** - Click **Enabled**.
- **Aggregate MSDU Max Length** - Type **4096**.
- **Aggregate MPDU** - Click **Enabled**.
- **Aggregate MPDU Max Length** - Click **Enabled**.
- **Agg. MPDU Max # of Sub-frames** - Type **64**.
- **ADDBA Support** - Click **Enabled**.

5 From the main menu, click **WM Access Domain**. The **WM Access Domain Configuration** page is displayed.

6 In the left pane **WM Access Domain**s list, click the WM-AD you want to configure. The **Topology** tab is displayed.

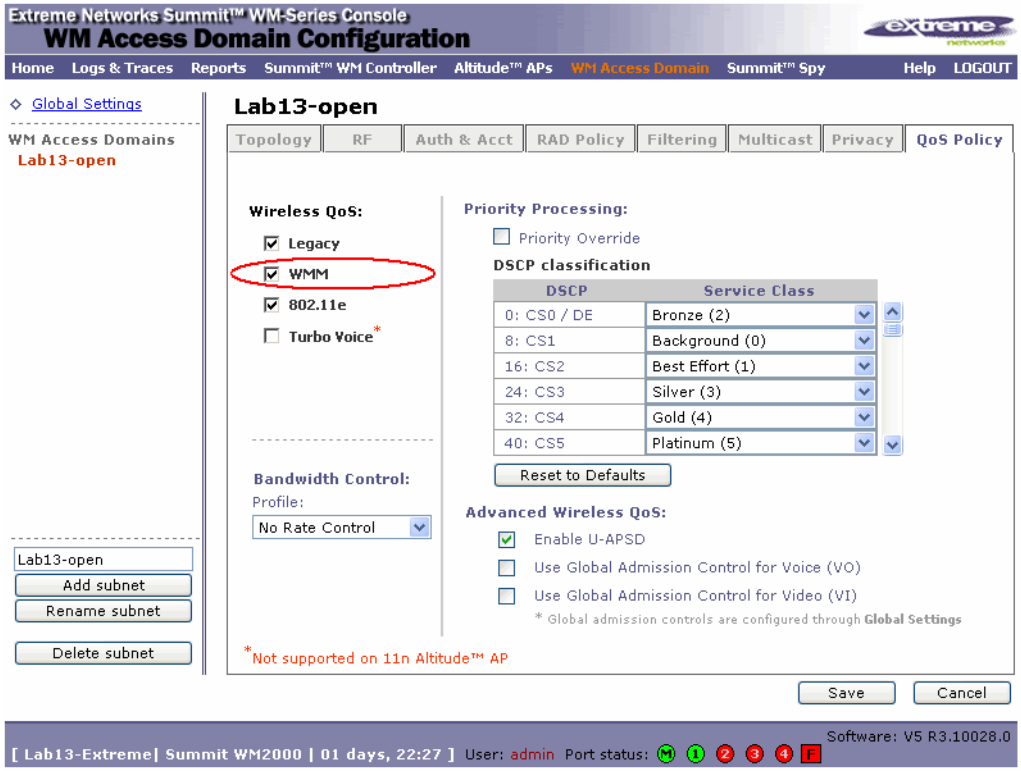
7 Click the **Privacy** tab. Some client devices will not use 802.11n mode if they are using WEP or TKIP for security. Therefore, do one of the following:

- Select **None**.
- Select **WPA-PSK**, and then clear the **WPA v.1** option:
  - Select **WPA v.2**.
  - In the **Encryption** drop-down list, click **AES only**.



8 Click the **QoS Policy** tab.

9 In the **Wireless QoS** section, select the **WMM** option. Some 802.11n client devices will remain at 54Mbps unless WMM is enabled.



Modifying Altitude AP 350-2i/350-2d radio properties

The following section discusses how to modify an Altitude AP 350-2i/350-2d and the Outdoor AP. For information on how to modify an Altitude 802.11n AP 450/451, see "Modifying Altitude 802.11n AP 450/451 radio properties" on page 90.

To modify the Altitude AP's radio properties:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 Click the appropriate Altitude AP in the list.

3 Click the radio tab you want to modify.

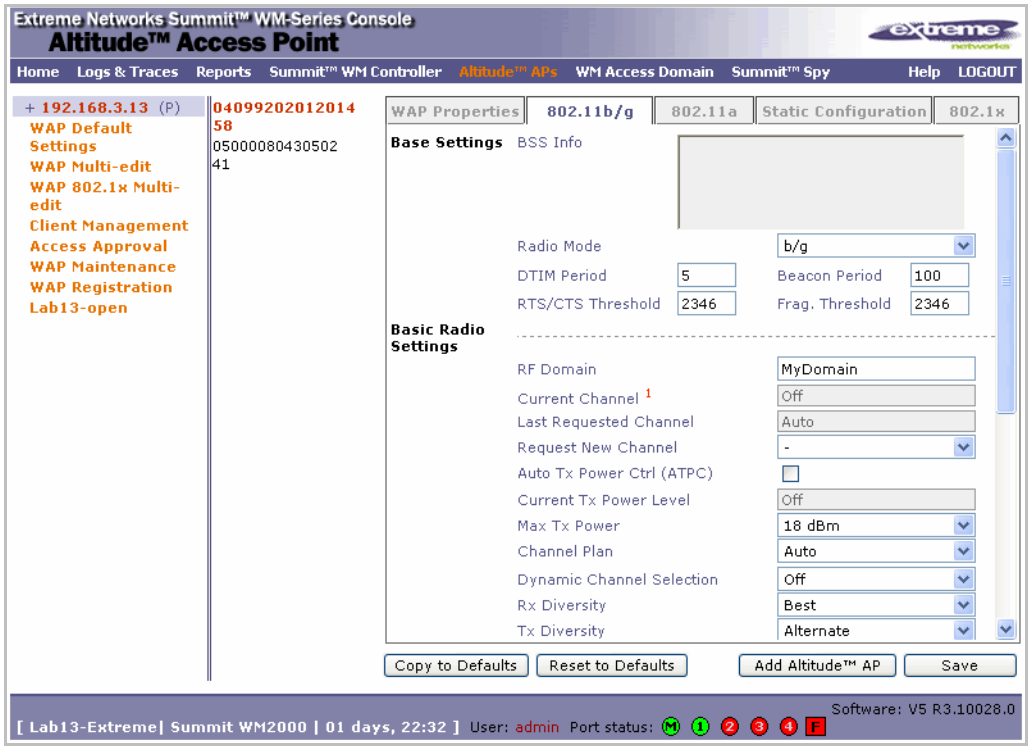
Each tab displays the radio settings for each radio on the Altitude AP. If the radio has been assigned to a WM-AD, the WM-AD names and MAC addresses appear in the **Base Settings** section. The Summit WM Controller can support the following:

- WM200/2000 - Up to 64 WM-ADs
- WM20 - Up to 8 WM-ADs
- WM1000 - Up to 50 WM-ADs
- WM100 - Up to 32 WM-ADs

The Altitude AP radios can be assigned to each of the configured WM-ADs in a system. Each radio can be the subject of 8 WM-AD assignments (corresponding to the number of SSIDs it can support). Once a radio has all 8 slots assigned, it is no longer eligible for further assignment.

The **BSS Info** section is view only. After WM-AD configuration, the **Basic Service Set (BSS)** section displays the MAC address on the Altitude AP for each WM-AD and the SSIDs of the WM-ADs to which this radio has been assigned.

4 If applicable, click the **802.11b/g** tab to modify the radio properties:



5 In the **Base Settings** section, do the following:

- **Radio Mode** - Click one of the following radio options:
  - **b** - Click to select the 802.11b-only mode of the 802.11b/g radio. If selected, the AP will use only 11b (CCK) rates with all associated clients. The AP will not transmit or receive 11g rates.
  - **g** - Click to select the 802.11g-only mode of the 802.11b/g radio. If selected, the AP will not accept associations from 11b clients, but it will still use all CCK and OFDM 11g rates with its associated clients. To disable CCK rates, use the **Min/Max Basic Rate** and **Max Operation Rate** controls to select OFDM-only rates.
  - **b/g** - Click to enable both the 802.11g mode and the 802.11b mode of the 802.11b/g radio. If selected, the AP will accept associations from all clients and use all available 11b and 11g rates.
  - **off** - Click to disable the 802.11b/g radio.
- **DTIM Period** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** - Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** - Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.

- **Frag. Threshold** - Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

6 In the **Basic Radio Settings** section, do the following:

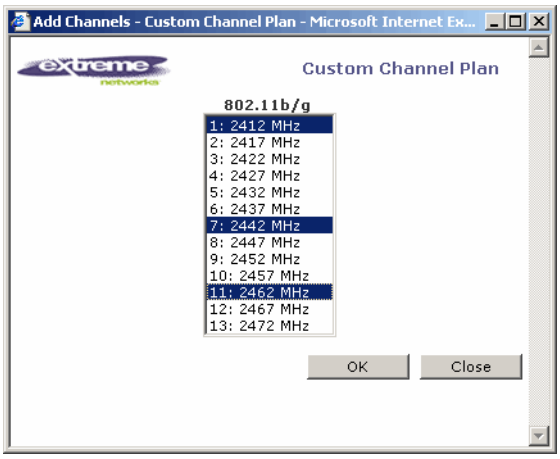
- **RF Domain** - Type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 16 characters. The RF Domain is used to identify a group of Altitude APs.
- **Current Channel** - This field is view only. It displays the actual channel the ACS has assigned to the Altitude AP radio. The **Current Channel** value and the **Last Requested Channel** value may be different because the ACS automatically assigns the best available channel to the Altitude AP, ensuring that an Altitude AP's radio is always operating on the best available channel.
- **Last Requested Channel** - This field is view only. This field displays the last wireless channel that you had selected for the Altitude AP to communicate with the wireless devices.
- **Request New Channel** - Click the wireless channel you want the Altitude AP to use to communicate with wireless devices.
  Click **Auto** to request the ACS to search for a new channel for the Altitude AP, using a channel selection algorithm. This forces the AP to go through the auto-channel selection process again. Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information".
- **Auto Tx Power Ctrl (ATPC)** - Select to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.
- **Current Tx Power Level** - This field is view only. It displays the actual Tx power level assigned to the Altitude AP radio.
- **Max Tx Power** - Click the maximum Tx power level that the range of transmit power can be adjusted: **8 to 18 dBm**. It is recommended to use **18 dBm** to not limit the potential Tx power level range that can be used.
- **Min Tx Power** - If ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted. It is recommended to use the lowest value available to not limit the potential Tx power level range that can be used.

NOTE

The Minimum Tx Power level is subject to the regulatory compliance requirement for the selected country.

- **Auto Tx Power Ctrl Adjust** - If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to click **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Channel Plan** - If ACS is enabled, you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference. Click one of the following:
  - **3 Channel Plan** - ACS will scan the following channels: 1, 6, and 11 in the US, and 1, 7, and 13 in Europe.
  - **4 Channel Plan** - ACS will scan the following channels: 1, 4, 7, and 11 in the US, and 1, 5, 9, and 13 in Europe.

- **Auto** - ACS will scan the default channel plan channels: 1, 6, and 11 in the US, and 1, 5, 9, and 13 in Europe.
- **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.



- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger ACS.
- **Rx Diversity** - Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** - Click **Alternate** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Alternate** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Alternate**. Under those circumstances, it is recommended to use either **Left** or **Right** for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Alternate** if two identical antennas are not used.
- **Min Basic Rate** - Click the minimum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the

Min Basic Rate. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.

- **Max Basic Rate** - Click the maximum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Operational Rate** - Click the maximum data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, or **11** Mbps for 11b-only mode. Click **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **28**, or **54** Mbps for 11b+11g or 11g-only modes. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **No of Retries for Background BK** - Click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Best Effort BE** - Click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)** The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Video VI** - Click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Voice VO** - Click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Turbo Voice TVO** - Click the number of retries for the Turbo Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.

7 In the **11b Settings** section, do the following:

- **Preamble** - Click a preamble type for 11b-specific (CCK) rates: **Short** or **Long**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.

8 In the **11g Settings** section, do the following:

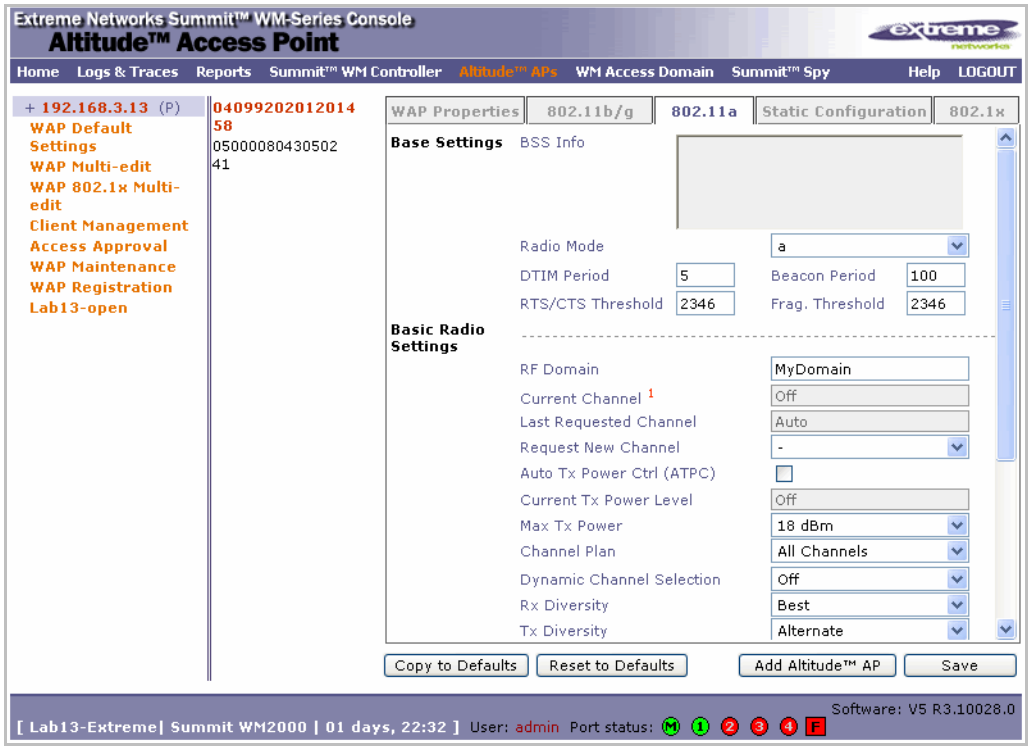
- **Protection Mode** - Click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **Protection Rate** - Click a protection rate: **1**, **2**, **5.5**, or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.
- **Protection Type** - Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

NOTE

*The overall throughput is reduced when **Protection Mode** is enabled, due to the additional overhead caused by the RTS/CTS. The overhead is minimized by setting **Protection Type** to **CTS Only** and **Protection Rate** to **11 Mbps**. Although, the overhead causes the overall throughput to be sometimes lower than if just 11b mode is used. If there are many 11b clients, it is recommended to disable 11g support (11g clients are backward compatible with 11b APs).*

An alternate approach, although a more expensive method, is to dedicate all APs on a channel for 11b (for example, disable 11g on these APs) and disable 11b on all other APs. The difficulty with this method is that the number of APs must be increased to ensure coverage separately for 11b and 11g clients.

9 If applicable, click the **802.11a** tab to modify the radio properties:



10 In the **Base Settings** section, do the following:

- **Radio Mode** - Click one of the following radio options:
  - **a** - Click to enable the 802.11a radio.
  - **off** - Click to disable the 802.11a radio.
- **DTIM Period** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** - Type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS Threshold** - Type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** - Type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.

11 In the **Basic Radio Settings** section, do the following:

- **RF Domain** - Type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 16 characters. The RF Domain is used to identify a group of Altitude APs.
- **Current Channel** - This field is view only. It displays the actual channel the ACS has assigned to the Altitude AP radio. The Current Channel value and the Requested Channel value may be different because the ACS automatically assigns the best available channel to the Altitude AP, ensuring that an Altitude AP's radio is always operating on the best available channel.

- **Last Requested Channel** - This field displays the last wireless channel that you had selected for the Altitude AP to communicate with the wireless devices.
- **Requested New Channel** - Click the wireless channel you want the Altitude AP to use to communicate with wireless devices.

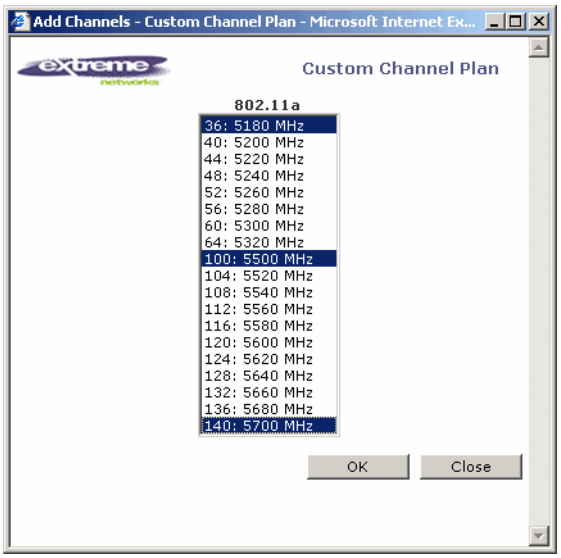
  Click **Auto** to request the ACS to search for a new channel for the Altitude APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again.

  Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information."
- **Auto Tx Power Ctrl (ATPC)** - Click to enable ATPC. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.
- **Current Tx Power Level** - This field is view only. It displays the actual Tx power level assigned to the Altitude AP radio.
- **Max Tx Power** - Click the maximum Tx power level that the range of transmit power can be adjusted: **0** to **18** dBm. It is recommended to use **18 dBm** to not limit the potential Tx power level range that can be used.
- **Min Tx Power** - If ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted. It is recommended to use the lowest value available to not limit the potential Tx power level range that can be used.

NOTE

The Minimum Tx Power level is subject to the regulatory compliance requirement for the selected country

- **Auto Tx Power Ctrl Adjust** - If ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Channel Plan** - If ACS is enabled, you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference. Click one of the following:
  - **All Channels** - ACS will scan all the channels for an operating channel.
  - **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.



- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger **ACS**.
- **Rx Diversity** - Click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default and recommended selection is **Best**. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** - Click **Alternate** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity antennas. The default selection is **Alternate** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Alternate**. Under those circumstances, it is recommended to use either **Left** or **Right** for Tx Diversity. If only one antennae is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Alternate** if two identical antennas are not used.
- **Min Basic Rate** - Click the minimum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.

- **Max Basic Rate** - Click the maximum data rate that must be supported by all stations in a BSS: **6**, **12**, or **24** Mbps. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Max Operational Rate** - Click the maximum data rate that clients can operate at while associated with the AP: **6**, **9**, **12**, **18**, **24**, **36**, **48**, or **54** Mbps. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Max Basic Rate**.

NOTE

Radio a channels 100 to 140 occupy the 5470-5725 MHz band in the regulatory domains of the European Union and European Union free trade countries.
Radio B/G Channels 12 and 13 are not available in North America. Radio B/G channel 14 is only available in Japan.

- **No of Retries for Background BK** - Click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Best Effort BE** - Click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Video VI** - Click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Voice VO** - Click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **No of Retries for Turbo Voice TVO** - Click the number of retries for the Turbo Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.

12 To save your changes, click **Save.**

Setting up the Altitude AP using static configuration

The Altitude AP static configuration feature provides the Summit WM Controller, Access Points, and WM software solution with the capability for a network with either a central office or a branch office model. The static configuration settings assist in the setup of branch office support. These settings are not dependent of branch topology, but instead can be employed at any time if required. In the branch office model, Altitude APs are installed in remote sites, while the Summit WM Controller is in the central office. The Altitude APs require the capability to interact in both the local site network and the central network. To achieve this model, a static configuration is used.

NOTE

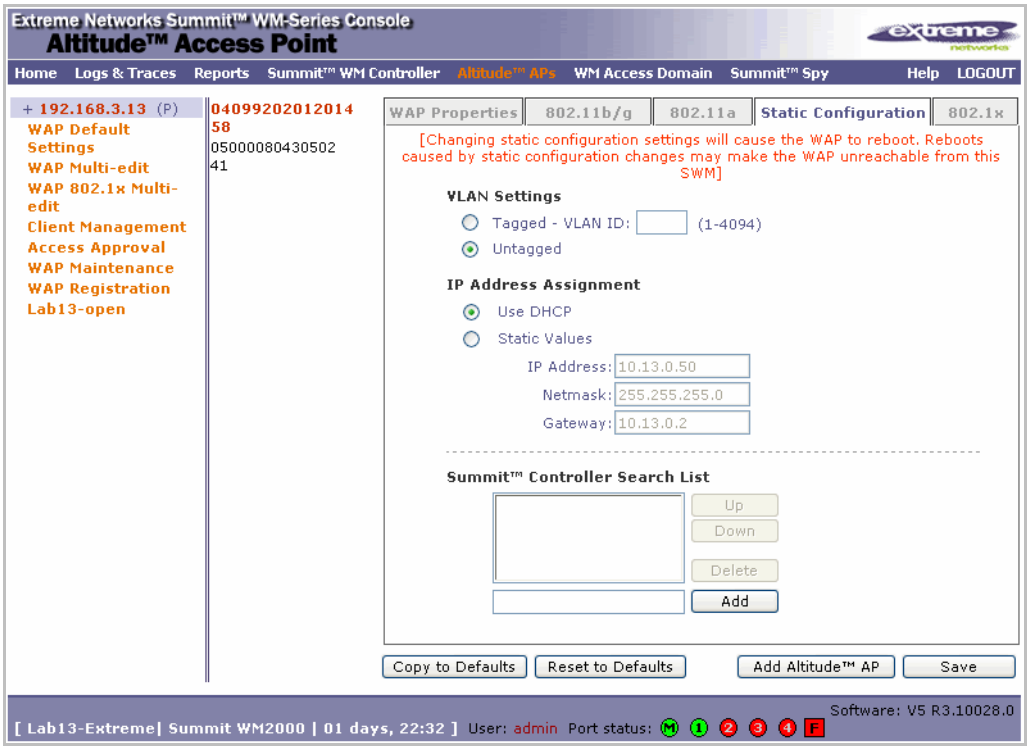
If an Altitude AP with a statically configured IP address (without a statically configured Wireless Controller Search List) cannot register with the Summit WM Controller within the specified number of retries, the Altitude AP will use SLP, DNS, and SLP multicast as a backup mechanism.

To set up a Altitude AP using static configuration:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 Click the appropriate Altitude AP in the list.

3 Click the **Static Configuration** tab.



4 Select one of the VLAN settings for the Altitude AP:

- **Tagged - VLAN ID** - Select if you want to assign this AP to a specific VLAN and type the value in the box.
- **Untagged** - Select if you want this AP to be untagged. This option is selected by default.

CAUTION

Caution should be exercised when using this feature. If a VLAN tag is not configured properly, the connectivity with the AP will be lost. To configure the AP VLAN, do the following:
- Connect the AP to the Summit WM Controller or to the network point that does not require AP VLAN tagging.
- Use Static Configuration to enable VLAN and define the VLAN ID.
- Save the configuration on the AP. The AP reboots and looses connectivity to the Summit WM Controller.
- Disconnect the AP and attach it to its final network location.
If the VLAN settings match the network configuration, the AP registers with the Summit WM Controller successfully. If the AP VLAN is not configured properly (wrong tag), connecting to the AP may not be possible. To recover from this situation, you will need to reset the AP to its factory default settings. For more information, see the Summit WM Maintenance Guide.

5 Select one of the two methods of IP address assignment for the Altitude AP:

- **Use DHCP** - Select this option to enable Dynamic Host Configuration Protocol (DHCP). This option is enabled by default.
- **Static Values** - Select this option to specify the IP address of the Altitude AP.
  - **IP Address** - Type the IP address of the AP.
  - **Subnet Mask** - Type the appropriate subnet mask to separate the network portion from the host portion of the address.
  - **Gateway** - Type the default gateway of the network.

NOTE

For the initial configuration of an Altitude AP to use a static IP address assignment, the following is recommended:
- Allow the Altitude AP to first obtain an IP address using DHCP. By default, Altitude APs are configured to use the DHCP IP address configuration method.
- Allow the Altitude AP to connect to the Summit WM Controller using the DHCP assigned IP address.
- After the Altitude AP has successfully registered to the Summit WM Controller, use the ***Static Configuration*** *tab to configure a static IP address for the Altitude AP, and then save the configuration.*
- Once the static IP address has been configured on the Altitude AP, the Altitude AP can then be moved to its target location, if applicable. (A branch office scenario is an example of a setup that may require static IP assignment.) If the Altitude AP IP address is not configured properly, connecting to the Altitude AP may not be possible. To recover from this situation, you will need to reset the Altitude AP to its factory default settings. For more information, see the Summit WM Maintenance Guide.

6 In the **Add** box, type the IP address of the Summit WM Controller that will control this Altitude AP.

7 Click **Add**. The IP address is added to the list.

8 Repeat steps 5 and 6 to add additional Summit WM Controllers.

9 Click **Up** and **Down** to modify the order of the Summit WM Controllers. The maximum is three controllers.

The Altitude AP attempts to connect to the IP addresses in the order in which they are listed. The Altitude AP is successful when it finds a Summit WM Controller that will allow it to register.

This feature allows the Altitude AP to bypass the discovery process. If the **Summit Controller Search List** box is not populated, the Altitude AP will use SLP to discover a Summit WM Controller.

For the initial Altitude AP deployment, it is necessary to use one of the described options in "Discovery and registration overview" on page 71.

10 To save your changes, click **Save**.

Setting up 802.1X authentication for an Altitude AP

802.1X is an authentication standard for wired and wireless LANs. The 802.1X standard can be used to authenticate access points to the LAN to which they are connected. 802.1X support provides security for network deployments where access points are placed in public areas.

To successfully set up 802.1X authentication of an Altitude AP, the Altitude AP must be configured for 802.1X authentication before the Altitude AP is connected to a 802.1X enabled switch port.

Certain LAN switches when enabled for 802.1X authentication, may not allow traffic from multiple supplicants once the AP is authenticated with the switch port. That means traffic from wireless clients associated with the Access Point would be blocked by the switch port. In such cases the Access point can only tunnel the client traffic to the Summit WM controller but will not be able to bridge it at the AP.

CAUTION

If the switch port, to which the Altitude AP is connected to, is not 802.1X enabled, the 802.1X authentication will not take effect.

802.1X authentication credentials can be updated at any time, whether or not the Altitude AP is connected with an active session. If the Altitude AP is connected, the new credentials are sent

immediately. If the Altitude AP is not connected, the new credentials are delivered the next time the Altitude AP connects to the Summit WM Controller.

There are two main aspects to the 802.1X feature:

- Credential management - The Summit WM Controller and the Altitude AP are responsible for the requesting, creating, deleting, or invalidating the credentials used in the authentication process.
- Authentication - The Altitude AP is responsible for the actual execution of the EAP-TLS or PEAP protocol.

802.1X authentication can be configured on a per access point basis. For example, 802.1X authentication can be applied to specific Altitude APs individually or with a multi-edit function.

The 802.1X authentication supports two authentication methods:

- PEAP (Protected Extensible Authentication Protocol)
  - Is the recommended 802.1X authentication method
  - Requires minimal configuration effort and provides equal authentication protection to EAP-TLS
  - Uses user ID and passwords for authentication of access points
- EAP-TLS
  - Requires more configuration effort
  - Requires the use of a third-party Certificate Authentication application
  - Uses certificates for authentication of access points
  - Summit WM Controller can operate in either proxy mode or pass through mode.
    - Proxy mode - The Summit WM Controller generates the public and private key pair used in the certificate.
    - Pass through mode - The certificate and private key is created by the third-party Certificate Authentication application.

NOTE

Although an Altitude AP can support using both PEAP and EAP-TLS credentials simultaneously, it is not recommended to do so. Instead, it is recommended that only one type of authentication be used, and that only credentials for that type of authentication get installed on the Altitude AP.

Configuring 802.1X PEAP authentication

PEAP authentication uses user ID and passwords for authentication. To successfully configure 802.1X authentication of an Altitude AP, the Altitude AP must first be configured for 802.1X authentication before the Altitude AP is deployed on a 802.1X enabled switch port.

NOTE

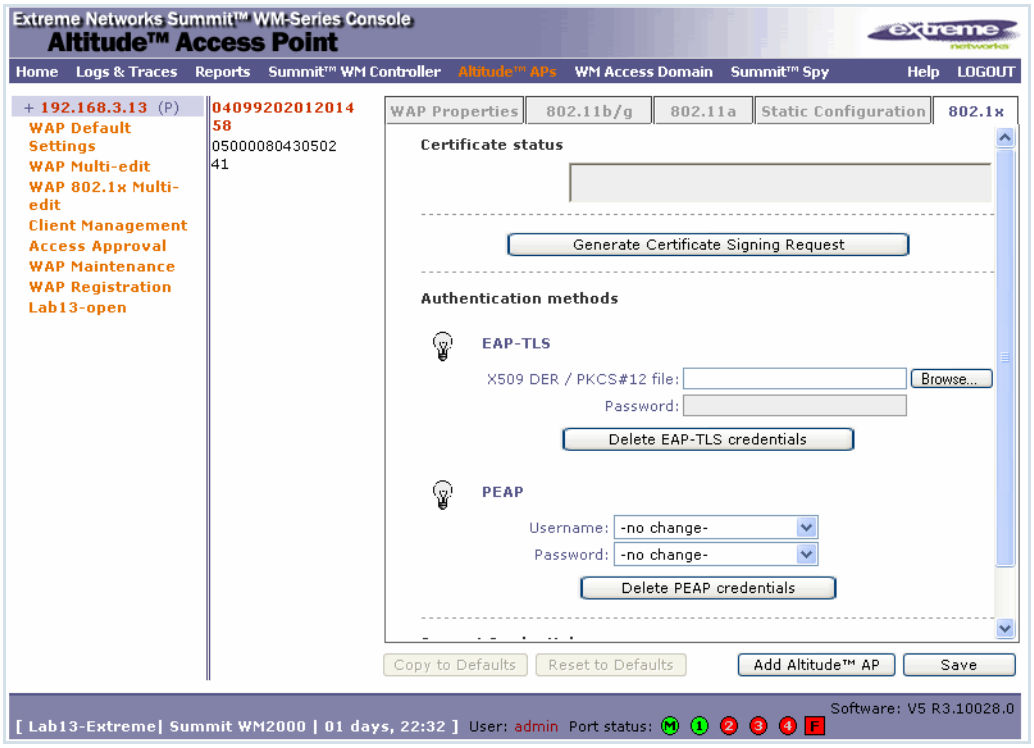
Usernames and passwords for PEAP authentication credentials each have a maximum length of 128 characters.

To configure 802.1X PEAP authentication:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the Altitude AP list, click the Altitude AP for which you want to configure 802.1X PEAP authentication.

3 Click the **802.1X** tab.



4 In the **Username** drop-down list, click the value you want to assign as the username credential:

- **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
- **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
- **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.
- **Other** - Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the username credential.

5 In the **Password** drop-down list, click the value you want to assign as the password credential:

- **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
- **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
- **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.
- **Other** - Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the password credential.

6 To save your changes, click **Save.**

The 802.1X PEAP authentication configuration is assigned to the Altitude AP. The Altitude AP can now be deployed to a 802.1X enabled switch port.

Configuring 802.1X EAP-TLS authentication

EAP-TLS authentication uses certificates for authentication. A third-party Certificate Authentication application is required to configure EAP-TLS authentication. Certificates can be overwritten with new ones at any time.

With EAP-TLS authentication, the Summit WM Controller can operate in either proxy mode or pass through mode.

NOTE

When an Altitude AP configured with 802.1X EAP-TLS authentication is connected to a Summit WM Controller, the Altitude AP begins submitting logs to the Summit WM Controller 30 days before the certificate expires to provide administrators with a warning of the impending expiry date.

Proxy mode

In proxy mode, Summit WM Controller generates the public and private key pair used in the certificate. You can specify the criteria used to create the Certificate Request. The Certificate Request that is generated by the Summit WM Controller is then used by the third-party Certificate Authentication application to create the certificate used for authentication of the Altitude AP. To successfully configure 802.1X authentication of an Altitude AP, the Altitude AP must first be configured for 802.1X authentication before the Altitude AP is deployed on a 802.1X enabled switch port.

To configure 802.1X EAP-TLS authentication in proxy mode:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the Altitude AP list, click the Altitude AP for which you want to configure 802.1X EAP-TLS authentication.

3 Click the **802.1X** tab.

4 Click **Generate certificate request**. The **Generate Certificate Request** window is displayed.

5 Type the criteria to be used to create the certificate request. All fields are required:

- **Country name** - The two-letter ISO abbreviation of the name of the country
- **State or Province name** - The name of the State/Province

- **Locality name (city)** - The name of the city
- **Organization name** - The name of the organization
- **Organizational Unit name** - The name of the unit within the organization
- **Common name** - Click the value you want to assign as the common name of the Altitude AP:
  - **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
  - **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
  - **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.
  - **Other** - Click to specify a custom value. A text box is displayed. In the text box, type the value you want to assign as the common name of the Altitude AP.
- **Email address** - The email address of the organization

6 Click **Generate certificate request**. A certificate request file is generated (.csr file extension). The name of the file is the Altitude AP serial number. The **File Download** dialog is displayed.

7 Click **Save**. The **Save as** window is displayed.

8 Navigate to the location on your computer that you want to save the generated certificate request file, and then click **Save**.

9 In the third-party Certificate Authentication application, use the content of the generated certificate request file to generate the certificate file (.cer file extension).

10 On the **802.1X** tab, click **Browse**. The **Choose file** window is displayed.

11 Navigate to the location of the certificate file, and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.

12 To save your changes, click **Save.**

The 802.1X EAP-TLS (certificate and private key) authentication in proxy mode is assigned to the Altitude AP. The Altitude AP can now be deployed to a 802.1X enabled switch port.

Pass through mode

In pass through mode, the certificate and private key is created by the third-party Certificate Authentication application. To successfully configure 802.1X authentication of an Altitude AP, the Altitude AP must first be configured for 802.1X authentication before the Altitude AP is deployed on a 802.1X enabled switch port.

Before you configure 802.1X using EAP-TLS authentication in pass through mode, you must first create a certificate using the third-party Certificate Authentication application and save the certificate file in PKCS #12 file format (.pfx file extension) on your system.

To configure 802.1X EAP-TLS authentication in pass through mode:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the Altitude AP list, click the Altitude AP for which you want to configure 802.1X EAP-TLS authentication.

3 Click the **802.1X** tab.

4 Click **Browse**. The **Choose file** window is displayed.

5 Navigate to the location of the certificate file (.pfx) and click **Open**. The name of the certificate file is displayed in the **X509 DER / PKCS#12 file** box.

6 In the **Password** box, type the password that was used to protect the private key.

NOTE

The password that was used to protect the private key must be a maximum of 31 characters long.

7 To save your changes, click **Save.**

The 802.1X EAP-TLS authentication in pass through mode is assigned to the Altitude AP. The Altitude AP can now be deployed to a 802.1X enabled switch port.

Viewing 802.1X credentials

When 802.1X authentication is configured on an Altitude AP, the light bulb icon on the **802.1X** tab for the configured Altitude AP is lit to indicate which 802.1X authentication method is used. An Altitude AP can be configured to use both EAP-TLS and PEAP authentication methods. For example, when both EAP-TLS and PEAP authentication methods are configured for the Altitude AP, both light bulb icons on the **802.1X** tab are lit.

NOTE

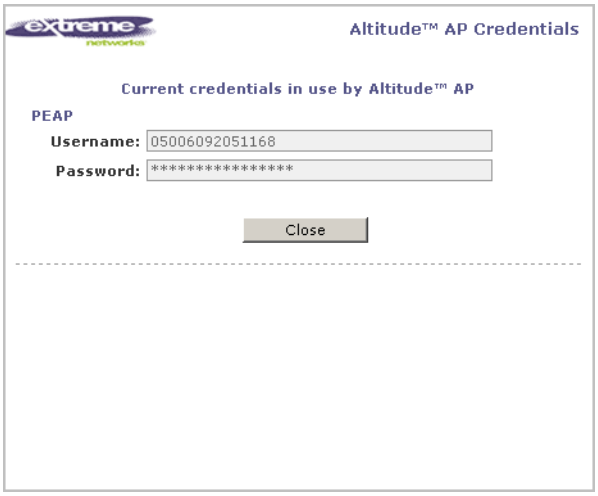
You can only view the 802.1X credentials of Altitude APs that have an active session with the Summit WM Controller. If you attempt to view the credentials of an Altitude AP that does not have an active session, the Altitude AP Credentials window displays the following message: ***Unable to query Altitude AP: not connected****.*

To view current 802.1X credentials:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the Altitude AP list, click the Altitude AP for which you want to view its current 802.1X credentials.

3 In the **Current Credentials** section, click **Get additional Certificate info**. The Altitude AP Credentials window is displayed.



Deleting 802.1X credentials

CAUTION

Exercise caution when deleting 802.1X credentials. For example, deleting 802.1X credentials may prevent the Altitude AP from being authenticated or to lose its connection with the Summit WM Controller.

To delete current 802.1X credentials:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the Altitude AP list, click the Altitude AP for which you want to delete its current 802.1X credentials.

3 Do the following:

- To delete EAP-TLS credentials, click **Delete EAP-TLS** credentials.
- To delete PEAP credentials, click **Delete PEAP** credentials.

The credentials are deleted and the Altitude AP settings are updated.

NOTE

If you attempt to delete the 802.1X credentials of an Altitude AP that currently does not have an active session with the Summit WM Controller, the credentials are only deleted after the Altitude AP connects with the Summit WM Controller.

Setting up 802.1X authentication for Altitude APs using Multi-edit

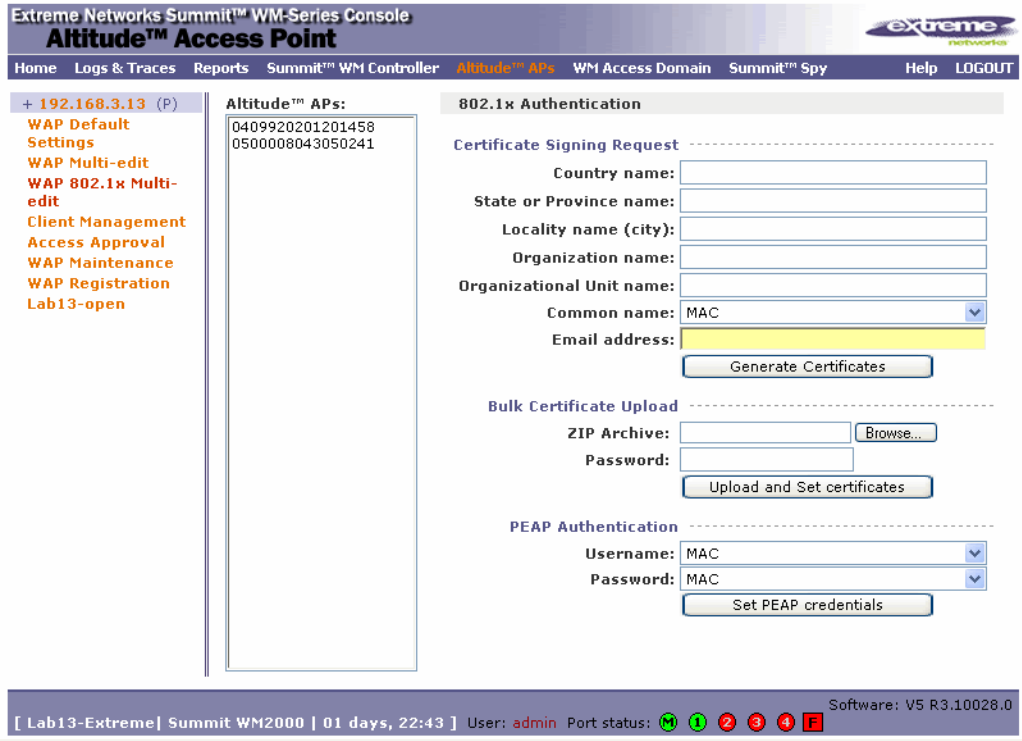
In addition to configuring Altitude APs individually, you can also configure 802.1X authentication for multiple Altitude APs simultaneously by using the AP 802.1X Multi-edit feature.

To configure 802.1X PEAP authentication using Multi-edit:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **AP 802.1X Multi-edit**.

3 In the **Altitude APs** list, click one or more APs to edit. To select multiple APs, click the APs from the list while pressing the CTRL key.



4 In the **PEAP Authentication** section, do the following:

- In the **Username** drop-down list, click the value you want to assign as the username credential:
  - **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
  - **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
  - **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.
- In the **Password** drop-down list, click the value you want to assign as the password credential:
  - **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
  - **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
  - **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.

5 Click **Set PEAP credentials**. The **AP 802.1X Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **Settings updated** message is displayed in the footer of the Summit WM GUI.

The 802.1X PEAP authentication configuration is assigned to the Altitude APs. The Altitude APs can now be deployed to 802.1X enabled switch ports.

To configure 802.1X EAP-TLS authentication in proxy mode using multi-edit:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **AP 802.1X Multi-edit**.

3 In the **Altitude APs** list, click one or more Altitude APs to configure. To click multiple Altitude APs, click the Altitude APs from the list while pressing the CTRL key.

4 In the **Certificate request** section, type the following:
   - **Country name** - The two-letter ISO abbreviation of the name of the country
   - **State or Province name** - The name of the State/Province
   - **Locality name (city)** - The name of the city
   - **Organization name** - The name of the organization
   - **Organizational Unit name** - The name of the unit within the organization
   - **Common name** - Click the value you want to assign as the common name of the Altitude AP:
     - **Name** - The name of the Altitude AP, which is assigned on the **WAP Properties** tab. The Altitude AP name can be edited.
     - **Serial** - The serial number of the Altitude AP. The Altitude AP serial number cannot be edited.
     - **MAC** - The MAC address of the Altitude AP. The Altitude AP MAC address cannot be edited.
   - **Email address** - The email address of the organization
5 Click **Generate Certificates**. The **AP 802.1X Multi-edit progress** window is displayed, which provides the status of the configuration process. Once complete, the **File Download** dialog is displayed.
6 Click **Save**. The **Save as** window is displayed.
7 Navigate to the location on your computer that you want to save the generated **certificate_requests.tar** file, and then click **Save**.

   The **certificate_requests.tar** file contains a certificate request (.csr) file for each Altitude AP. For each certificate request, generate a certificate using the third-party Certificate Authentication application. Once complete, zip all the certificates files (.cer) into one .zip file.
8 In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.
9 Navigate to the location of the zipped certificates file, and then click **Open**. The name of the zipped certificates file is displayed in the **ZIP Archive** box.
10 Click **Upload and Set certificates**. Once complete, the **Settings updated** message is displayed in the footer of the Summit WM GUI.

Configuring 802.1X EAP-TLS authentication in pass through mode using Multi-edit:

Before you configure 802.1X EAP-TLS authentication in pass through mode using Multi-edit, the following prerequisites are required:

- You must first generate a certificate for each Altitude AP using the third-party Certificate Authentication application.
- When generating the certificates:
  - Use the Common name value (either Name, Serial, or MAC) of the Altitude AP to name each generated certificate.
  - Use a common password for each generated certificate.
  - All .pfx files created by the third-party Certificate Authentication application must be zipped into one file.

To configure 802.1X EAP-TLS authentication in pass through mode using Multi-edit:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **AP 802.1X Multi-edit**.

3 In the **Altitude APs** list, click one or more Altitude APs to configure. To click multiple Altitude APs, click the Altitude APs from the list while pressing the CTRL key.

4 In the **Bulk Certificate Upload** section, click **Browse**. The **Choose file** window is displayed.

5 Navigate to the location of the zipped certificates file, and then click **Open**. The name of the zipped certificates file is displayed in the **ZIP Archive** box.

6 In the **Password** box, type the password used during the certificates generation process.

7 Click **Upload and Set certificates**. Once complete, the **Settings updated** message is displayed in the footer of the Summit WM GUI.

Configuring the default Altitude AP settings

Altitude APs are added with default settings. You can modify the system's Altitude AP default settings, and then use these default settings to configure newly added Altitude APs. In addition, you can base the system's Altitude AP default settings on an existing Altitude AP configuration or have configured Altitude APs inherit the properties of the default Altitude AP configuration when they register with the system.

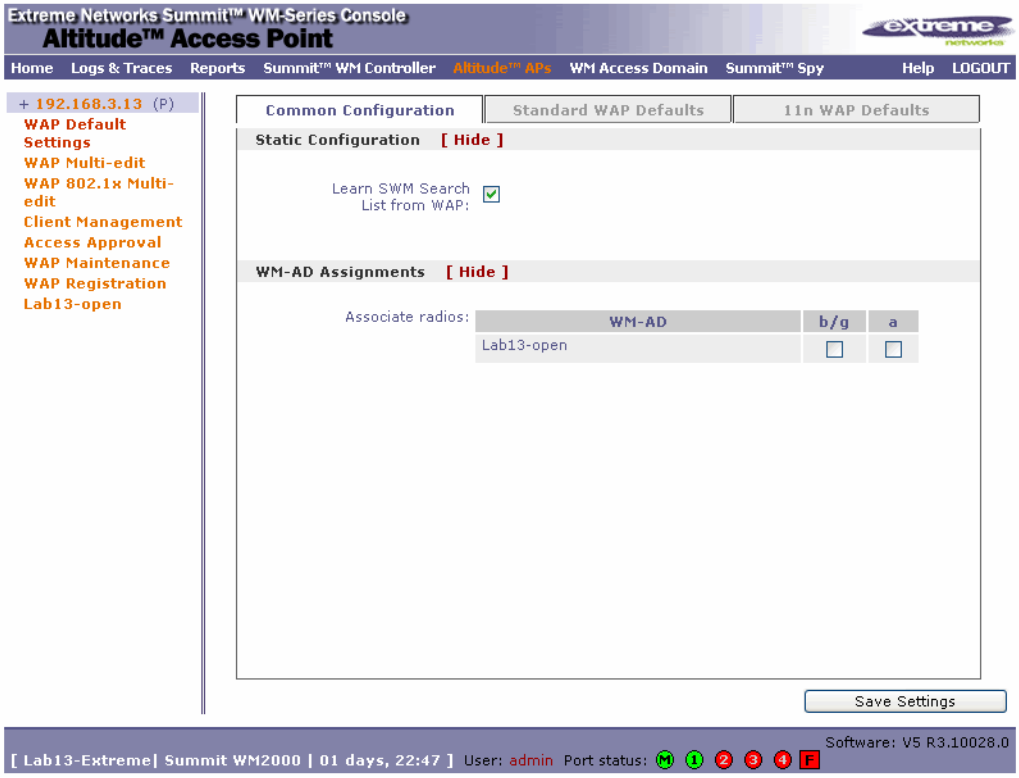
The process of configuring the default Altitude AP settings is divided into three tabs:

- **Common Configuration** - Configure common configuration, such as WM-AD assignments and static configuration options for all Altitude APs including, the Altitude AP 350-2i/350-2d, the Altitude 802.11n AP 450/451, and the Outdoor AP.
- **Standard AP Defaults** - Configure the default Altitude AP settings for only the Altitude AP 350-2i/350-2d and Outdoor AP.
- **11n AP Defaults** - Configure the default Altitude AP settings for only the Altitude 802.11n AP 450/451.

To configure the default AP settings:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **WAP Default Settings**.



3 Modify the following Altitude AP default settings as required:

- Static Configuration
- WM-AD Assignments
- WAP Properties
- Radio Settings

4 To configure common configuration applicable to all Altitude APs, click the **Common Configuration** tab.

5 In the **Static Configuration** section, do one of the following:

- To allow each Altitude AP to provide its own WM Search List, select the **Learn WM Search List from AP** checkbox.
- To specify a common WM Search List for all Altitude APs, clear the **Learn WM Search List from AP** checkbox, and then do the following:

a In the **Add** box, type the IP address of the Summit WM Controller that will control this Altitude AP.

b Click **Add**. The IP address is added to the list.

c Repeat steps **a** and **b** to add additional Summit WM Controllers.

d Click **Up** and **Down** to modify the order of the Summit WM Controllers. The maximum is three controllers.

The Altitude AP attempts to connect to the IP addresses in the order in which they are listed. The Altitude AP is successful when it finds a Summit WM Controller that will allow it to register.

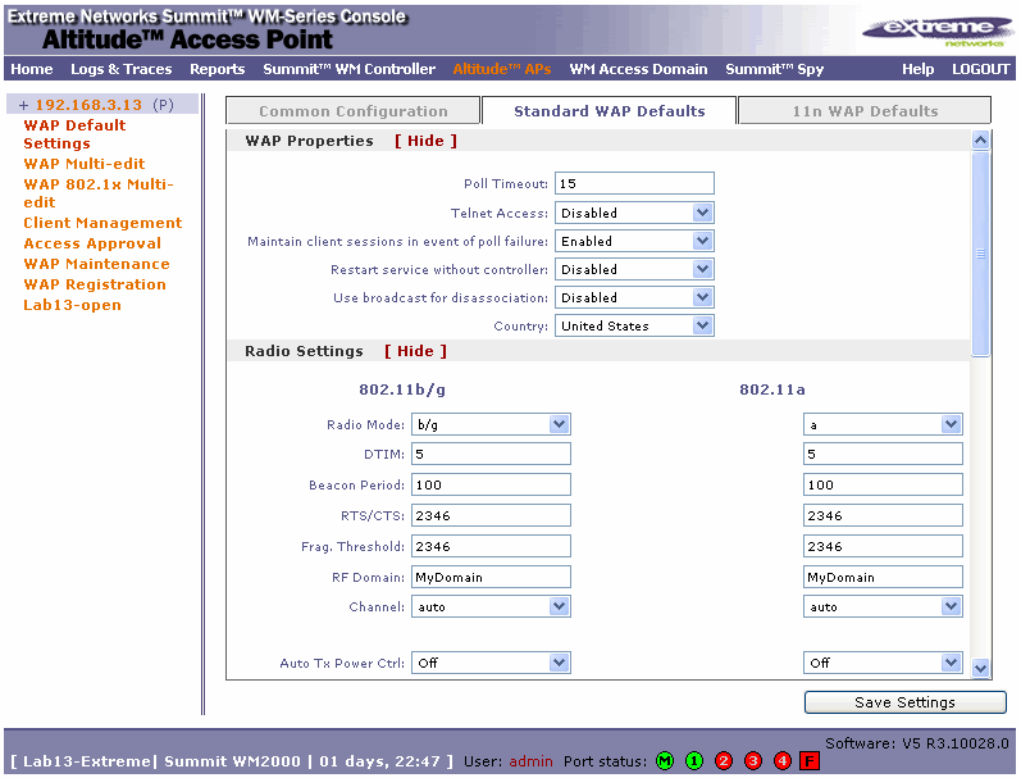
This feature allows the Altitude AP to bypass the discovery process. If the **Summit Controller Search List** box is not populated, the Altitude AP will use SLP to discover a Summit WM Controller.

The DHCP function for wireless clients must be provided locally by a local DHCP server, unless each wireless client has a static IP address.

For the initial Altitude AP deployment, it is necessary to use one of the described options in "Discovery and registration overview" on page 71.

6 In the **WM-AD Assignments** section, assign the radios for each WM-AD in the list by selecting or clearing the options.

7 To configure default Altitude AP settings for only the Altitude AP 350-2i/350-2d and Outdoor AP, click the **Standard WAP Defaults** tab.



8 In the **WAP Properties** section, do the following:

- **Poll Timeout** - Type the timeout value, in seconds. The Altitude AP uses this value to trigger re-establishing the link with the Summit WM Controller if it (Altitude AP) does not get an answer to its polling. The default value is 10 seconds.

NOTE

If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on WAP Properties screen. For more information, see "Session availability" on page 237.

- **Telnet Access** - Click whether Telnet Access to the Altitude AP is enabled or disabled.
- **Maintain client session in event of poll failure** - Select this option (if using a bridged at AP WM-AD) if the AP should remain active if a link loss with the controller occurs.This option is enabled by default.
- **Restart service in the absence of controller** - Select this option (if using a bridged at AP WM-AD) to ensure the Altitude APs' radios continue providing service if the Altitude AP's connection to the Summit WM Controller is lost. If this option is enabled, it allows the Altitude AP to start a bridged at AP WM-AD even in the absence of a Summit WM Controller.

- **Use broadcast for disassociation** - Select if you want the Altitude AP to use broadcast disassociation when disconnecting all clients, instead of disassociating each client one by one. This will affect the behavior of the AP under the following conditions:
  - If the Altitude AP is preparing to reboot or to enter one of the special modes (DRM initial channel selection).
  - If a BSSID is deactivated or removed on the Altitude AP.

  This option is enabled by default.
- **Country** - Click the country of operation. This option is only available with some licenses.

9 In the **Radio Settings** section, do the following:

- **Radio mode** - Click the radios you want to enable.
- **DTIM** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.
- **Beacon Period** - For each radio, type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS** - For each radio, type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** - For each radio, type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **RF Domain** - For each radio, type a string that uniquely identifies a group of APs that cooperate in managing RF channels and transmission power levels. The maximum length of the string is 16 characters. The RF Domain is used to identify a group of Altitude APs.
- **Channel** - For each radio, click the wireless channel you want the Altitude APs to use to communicate with wireless devices.
  Click **Auto** to request the ACS to search for a new channel for the Altitude APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again. If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm.
  Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information."
- **Auto Tx Power Ctrl** - For each radio, click to either enable or disable ATPC from the **Auto Tx Power Ctrl** drop-down list. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.
- **Max Tx Power** - For each radio, click the appropriate Tx power level from the **Max TX Power** drop-down list. The values in the **Max TX Power** drop-down is in dBm (dBm is an abbreviation for the power ratio in decibel (dB) of the measured power referenced to one milliwatt).
- **Min Tx Power** - For each radio, if ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted: **0** to **18** dBm. It is recommended to use **0 dBm** to not limit the potential Tx power level range that can be used.
- **Auto Tx Power Ctrl Adjust** - For each radio, if ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use **0 dBm** during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against

the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.

- **Channel Plan** - For each radio, if ACS is enabled you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.

  For radio b/g, click one of the following:

  - **3 Channel Plan** - ACS will scan the following channels: 1, 6, and 11 in the US, and 1, 7, and 13 in Europe.
  - **4 Channel Plan** - ACS will scan the following channels: 1, 4, 7, and 11 in the US, and 1, 5, 9, and 13 in Europe.
  - **Auto** - ACS will scan the default channel plan channels: 1, 6, and 11 in the US, and 1, 5, 9, and 13 in Europe.
  - **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click OK.

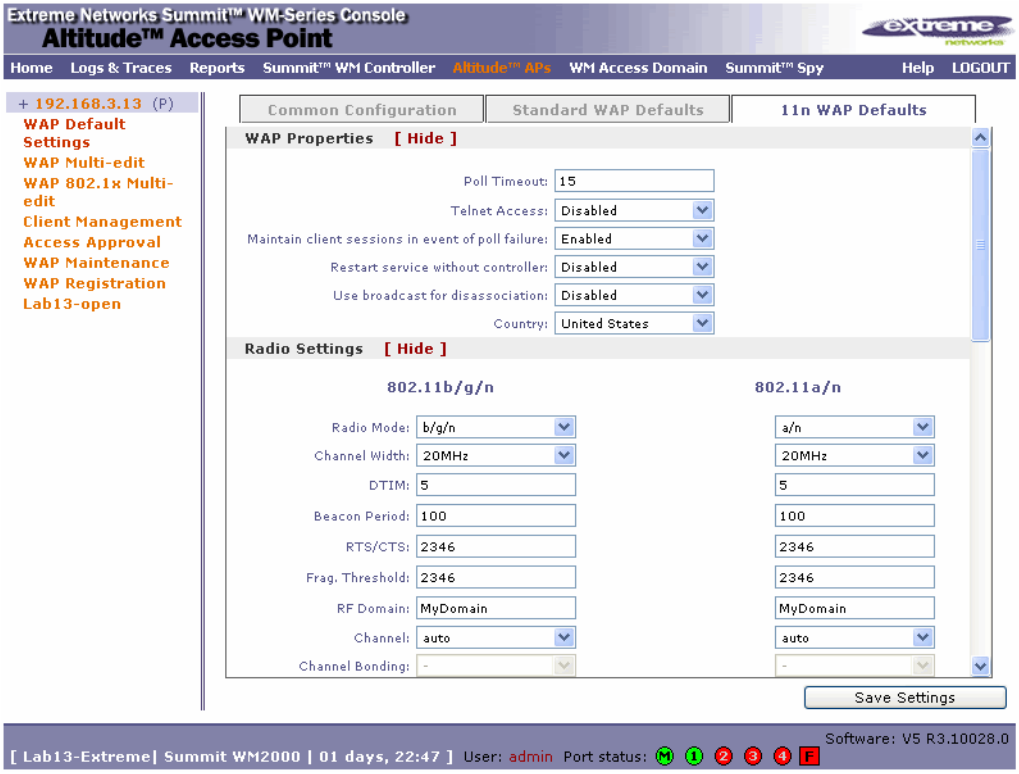
  For radio a, click one of the following:

  - **All Channels** - ACS will scan all the channels for an operating channel.
  - **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.
- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger **ACS.**
- **Rx Diversity** - For each radio, click **Best** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity receiving antennas. The default and recommended selection is **Best**. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Best** if two identical antennas are not used.
- **Tx Diversity** - For each radio, click **Alternate** for the best signal from both antennas, or **Left** or **Right** to choose either of the two diversity receiving antennas. The default selection is **Alternate** that maximizes performance for most clients. However, some clients may behave oddly with Tx Diversity set to **Alternate**. Under those circumstances, it is recommended to use either **Left** or

Right for Tx Diversity. If only one antenna is connected, use the corresponding **Left** or **Right** diversity setting. Do not use **Alternate** if two identical antennas are not used.

- **Preamble** - Click a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.
- **Protection Mode** - Click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **Protection Rate** - Click a protection rate: **1**, **2**, **5.5**, or **11** Mbps. The default and recommended setting is **11**. Only reduce the rate if there are many 11b clients in the environment or if the deployment has areas with poor coverage. For example, rates lower than **11** Mbps are required to ensure coverage.
- **Protection Type** - Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.
- **Min Basic Rate** - For each radio, click the minimum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. Click **6**, **12**, or **24** Mbps for 11a mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Basic Rate** - For each radio, click the maximum data rate that must be supported by all stations in a BSS: **1**, **2**, **5.5**, or **11** Mbps for 11b and 11b+11g modes. Click **1**, **2**, **5.5**, **6**, **11**, **12**, or **24** Mbps for 11g-only mode. Click **6**, **12**, or **24** Mbps for 11a mode. If necessary, the **Max Basic Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**. If both **Min Basic Rate** and **Max Basic Rate** are set to an 11g-specific (OFDM) rate, (for example, **6**, **12**, or **24** Mbps) all basic rates will be 11g-specific.
- **Max Operational Rate** - For each radio, click the maximum data rate that clients can operate at while associated with the AP: **1**, **2**, **5.5**, or **11** Mbps for 11b-only mode. Click **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **28**, or **54** Mbps for 11b+11g or 11g-only modes. Click **6**, **9**, **12**, **18**, **24**, **36**, **48**, or **54** Mbps for 11a mode. If necessary, the **Max Operational Rate** choices adjust automatically to be higher or equal to the **Min Basic Rate**.
- **Background BK** - For each radio, click the number of retries for the Background transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Best Effort BE** - For each radio, click the number of retries for the Best Effort transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Video VI** - For each radio, click the number of retries for the Video transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Voice VO** - For each radio, click the number of retries for the Voice transmission queue. The default value is **adaptive (multi-rate)**. The recommended setting is **adaptive (multi-rate)**.
- **Turbo Voice TVO** - For each radio, click the number of retries for the Turbo Voice transmission queue. The default value is **1**. The recommended setting is **adaptive (multi-rate)**.

10 To configure default Altitude AP settings for only the Altitude 802.11n AP 450/451, click the **11n WAP Defaults** tab.



11 In the **WAP Properties** section, do the following:

- **Poll Timeout** - Type the timeout value, in seconds. The Altitude AP uses this value to trigger re-establishing the link with the Summit WM Controller if it (Altitude AP) does not get an answer to its polling. The default value is 10 seconds.

NOTE

If you are configuring session availability, the Poll Timeout value should be 1.5 to 2 times of Detect link failure value on WAP Properties screen. For more information, see "Session availability" on page 237.

- **Telnet Access** - Click whether Telnet Access to the Altitude AP is enabled or disabled.
- **Country** - Click the country of operation. This option is only available with some licenses.

12 In the **Radio Settings** section, do the following:

- **Radio Mode** - Click the radios you want to enable.
- **Channel Width** - Click the channel width for the radio:
  - **20MHz** - Click to allow 802.11n clients to use the primary channel (20MHz) and non-802.11n clients, beacons, and multicasts to use the 802.11b/g radio protocols.
  - **40MHz** - Click to allow 802.11n clients that support the 40MHz frequency to use 40MHz, 20MHz, or the 802.11b/g radio protocols. 802.11n clients that do not support the 40MHz frequency can use 20MHz or the 802.11b/g radio protocols and non-802.11n clients, beacons, and multicasts use the 802.11b/g radio protocols.
  - **Auto** - Click to automatically switch between 20MHz and 40MHz channel widths, depending on how busy the extension channel is.
- **DTIM** - Type the desired DTIM (Delivery Traffic Indication Message) period - the number of beacon intervals between two DTIM beacons. To ensure the best client power savings, use a large

number. For example, 5. Use a small number to minimize broadcast and multicast delay. The default value is **5**.

- **Beacon Period** - For each radio, type the desired time, in milliseconds, between beacon transmissions. The default value is **100** milliseconds.
- **RTS/CTS** - For each radio, type the packet size threshold, in bytes, above which the packet will be preceded by an RTS/CTS (Request to Send/Clear to Send) handshake. The default value is **2346**, which means all packets are sent without RTS/CTS. Reduce this value only if necessary.
- **Frag. Threshold** - For each radio, type the fragment size threshold, in bytes, above which the packets will be fragmented by the AP prior to transmission. The default value is **2346**, which means all packets are sent unfragmented. Reduce this value only if necessary.
- **Channel** - For each radio, click the wireless channel you want the Altitude APs to use to communicate with wireless devices.
  Click **Auto** to request the ACS to search for a new channel for the Altitude APs, using a channel selection algorithm. This forces the APs to go through the auto-channel selection process again. If DRM is enabled (DRM is enabled by default), it scans automatically for a channel, using a channel selection algorithm.
  Depending on the regulatory domain (based on country), some channels may be restricted. The default value is based on North America. For more information, see Appendix B, "Regulatory information."
- **Channel Bonding** - Click the bonding method, **Up** or **Down**. The primary channel (20MHz) is bonded with an extension channel that is either 20MHz above (bonding up) or 20MHz below (bonding down) of the primary channel. Depending on the channel that is selected in the **Request New Channel** drop-down list, you may be prevented from bonding **Up** or **Down** in the **Channel Bonding** drop-down list.
- **Guard Interval** - Click a guard interval, **Long** or **Short**, when a 40MHz channel is used. It is recommended to use a short guard interval in small rooms (for example, a small office space) and a long guard interval in large rooms (for example, a conference hall).
- **Auto Tx Power Ctrl** - For each radio, click to either enable or disable ATPC from the **Auto Tx Power Ctrl** drop-down list. ATPC automatically adapts transmission power signals according to the coverage provided by the Altitude APs. After a period of time, the system will stabilize itself based on the RF coverage of your Altitude APs.
- **Max Tx Power** - For each radio, click the appropriate Tx power level from the **Max TX Power** drop-down list. The values in the **Max TX Power** drop-down is in dBm (dBm is an abbreviation for the power ratio in decibel (dB) of the measured power referenced to one milliwatt).
- **Min Tx Power** - For each radio, if ATPC is enabled, click the minimum Tx power level that the range of transmit power can be adjusted: 0 to 18 dBm. It is recommended to use 0 dBm to not limit the potential Tx power level range that can be used.
- **Auto Tx Power Ctrl Adjust** - For each radio, if ATPC is enabled, click the Tx power level that can be used to adjust the ATPC power levels that the system has assigned. It is recommended to use 0 dBm during your initial configuration. If you have an RF plan that recommended Tx power levels for each Altitude AP, compare the actual Tx power levels your system has assigned against the recommended values your RF plan has provided. Use the **Auto Tx Power Ctrl Adjust** value to achieve the recommended values.
- **Channel Plan** - For each radio, if ACS is enabled you can define a channel plan for the Altitude AP. Defining a channel plan allows you to limit which channels are available for use during an ACS scan. For example, you may want to avoid using specific channels because of low power, regulatory domain, or radar interference.

  For radio b/g/n, click one of the following:

- **3 Channel Plan** - ACS will scan the following channels: 1, 6, and 11 in the US, and 1, 7, and 13 in Europe.
- **4 Channel Plan** - ACS will scan the following channels: 1, 4, 7, and 11 in the US, and 1, 5, 9, and 13 in Europe.
- **Auto** - ACS will scan the default channel plan channels: 1, 6, and 11 in the US, and 1, 5, 9, and 13 in Europe.
- **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.

For radio a/n, click one of the following:

- **All Channels** - ACS will scan all the channels for an operating channel.
- **Custom** - If you want to configure individual channels from which the ACS will select an operating channel, click **Configure**. The **Add Channels** dialog is displayed. Click the individual channels you want to add to the channel plan while pressing the CTRL key, and then click **OK**.

- **Dynamic Channel Selection** - To enable Dynamic Channel Selection, click one of the following:
  - **Monitor Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated.
  - **Active Mode** - If traffic or noise levels exceed the configured DCS thresholds, an alarm is triggered and an information log is generated. In addition, the Altitude AP will cease operating on the current channel and ACS is employed to automatically select an alternate channel for the Altitude AP to operate on.
  - **DCS Noise Threshold** - Type the noise interference level, measured in dBms, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Channel Occupancy Threshold** - Type the channel utilization level, measured as a percentage, after which ACS will scan for a new operating channel for the Altitude AP if the threshold is exceeded.
  - **DCS Update Period** - Type the time, measured in minutes that determines the period during which the Altitude AP averages the **DCS Noise Threshold** and **DCS Channel Occupancy Threshold** measurements. If either one of these thresholds is exceeded, then the Altitude AP will trigger **ACS**.
- **Preamble** - Click a preamble type for 11b-specific (CCK) rates: **Short**, **Long**, or **Auto**. The recommended value is **Auto**. Click **Short** if you are sure that there is no pre-11b AP or a client in the vicinity of this AP. Click **Long** if compatibility with pre-11b clients is required.
- **Protection Mode** - Click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **Protection Type** - Click a protection type: **CTS Only** or **RTS CTS**. The default and recommended setting is **CTS Only**. Click **RTS CTS** only if an 11b AP that operates on the same channel is detected in the neighborhood, or if there are many 11b-only clients in the environment.

13 In the **11n Settings** section, do the following:

- **Protection Mode** - For each radio, click a protection mode: **None**, **Auto**, or **Always**. The default and recommended setting is **Auto**. Click **None** if 11b APs and clients are not expected. Click **Always** if you expect many 11b-only clients.
- **40MHz Protection Mode** - Click a protection type, **CTS Only** or **RTS- CTS**, or **None**, when a 40MHz channel is used. This protects high throughput transmissions on extension channels from interference from non-11n APs and clients.

- **40MHz Prot. Channel Offset** - Select a 20MHz channel offset if the deployment is using channels that are 20MHz apart (for example, using channels 1, 5, 9, and 13) or a 25MHz channel offset if the deployment is using channels that are 25MHz apart (for example, using channels 1, 6, and 11).
- **40MHz Channel Busy Threshold** - Type the extension channel threshold percentage, which if exceeded, will disable transmissions on the extension channel (40MHz).
- **Aggregate MSDUs** - Click an aggregate MSDU mode: **Enabled** or **Disabled**. Aggregate MSDU increases the maximum frame transmission size.
- **Aggregate MSDU Max Length** - Type the maximum length of the aggregate MSDU. The value range is 2290-4096 bytes.
- **Aggregate MPDUs** - Click an aggregate MPDU mode: **Enabled** or **Disabled**. Aggregate MPDU provides a significant improvement in throughput.
- **Aggregate MPDU Max Length** - Type the maximum length of the aggregate MPDU. The value range is 1024-65535 bytes.
- **Agg. MPDU Max # of Sub-frames** - Type the maximum number of sub-frames of the aggregate MPDU. The value range is 2-64.

14 **ADDBA Support** - Click an ADDBA support mode: **Enabled** or **Disabled**. ADDBA, or block acknowledgement, provides acknowledgement of a group of frames instead of a single frame. **ADDBA Support** must be enabled if **Aggregate APDU** is enable.

15 To save your changes, click **Save Settings**.

Modifying an Altitude AP's properties based on a default AP configuration

If you have an Altitude AP that is already configured with its own settings, but would like the Altitude AP to be reset to use the system's default AP settings, use the **Reset to Defaults** feature on the **WAP Properties** tab.

To configure an Altitude AP with the system's default AP settings:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to modify. The **WAP Properties** tab displays Altitude AP information.

3 To have the Altitude AP inherit the system's default AP settings, click **Reset to Defaults**. A pop-up window asking you to confirm the configuration change is displayed.

4 To confirm resetting the AP to the default settings, click **OK**.

Modifying the Altitude AP's default setting using the Copy to Defaults feature

You can modify the system's default AP settings by using the **Copy to Defaults** feature on the **WAP Properties** tab. This feature allows the properties of an already configured AP to become the system's default AP settings.

To modify the system's default AP settings based on an already configured AP:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the **Altitude AP** list, click the Altitude AP whose properties you want to become the system's default AP settings. The **WAP Properties** tab displays Altitude AP information.

3 If applicable, modify the Altitude AP's properties. For more information, see "Modifying an Altitude AP's properties" on page 86.

4 To make this AP's configuration be the system's default AP settings, click **Copy to Defaults**. A pop-up window asking you to confirm the configuration change is displayed.

5 To confirm resetting the system's default AP settings, click **OK**.

Configuring Altitude APs simultaneously

In addition to configuring Altitude APs individually, you can also configure multiple Altitude APs simultaneously by using the **AP Multi-edit** functionality. Configuring Altitude APs simultaneously is similar to modifying the system's default AP settings or individual Altitude APs.

When selecting the Altitude APs to simultaneously configure, you can use the following criteria:

- Select the Altitude APs by hardware type
- Select the Altitude APs individually

You can select multiple hardware types and individual Altitude APs by pressing the Ctrl key and selecting the hardware types and specific Altitude APs.

NOTE

Only settings and options supported by all of the selected hardware types are available for configuring.

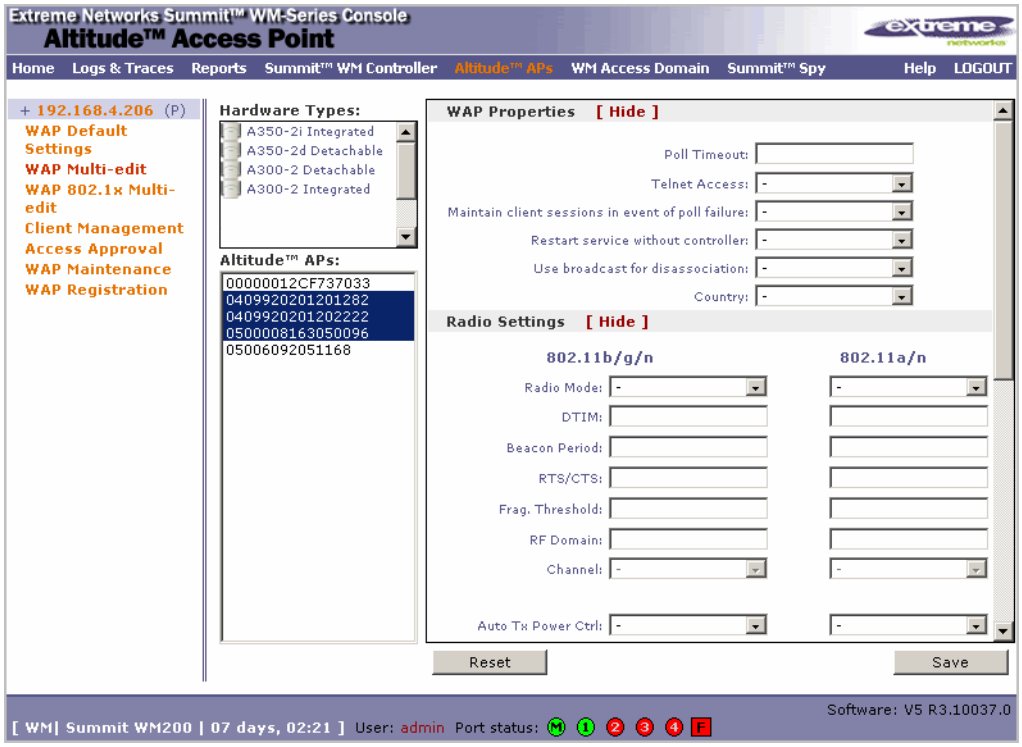
NOTE

When you configure multiple Altitude APs using the AP Multi-edit page, it is important to note that for some Altitude AP settings to be available for configuration, other Altitude AP settings must be enabled or configured first.

To configure Altitude APs simultaneously:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 In the left pane, click **WAP Multi-edit**.



3 Do the following:

- In the **Hardware Types** list, click one or more hardware types.
- In the **Altitude APs** list, click one or more Altitude APs to edit. To click multiple Altitude APs, click the APs from the list while pressing the CTRL key.

NOTE

When using multi-edit configuration, any box or option that is not explicitly modified will not be changed by the update.

*The Altitude APs shown in the **Altitude APs** list can be from any version of the software. Attributes that are common between software versions are set on all Altitude APs. Attributes that are not common, are only sent to the AP versions to which the attributes apply. Attempting to set an attribute that does not apply for an AP will not abort the multi-edit operation.*

4 Modify the configuration of the selected Altitude APs:

- **WAP Properties** - For more information, see "Modifying an Altitude AP's properties" on page 86.
- **Radio Settings** - For more information, see "Modifying Altitude AP radio properties" on page 88.
- **Static Configuration** - For more information, see "Setting up the Altitude AP using static configuration" on page 114.

5 In the **WAP Properties**, **Radio Settings**, and **Static Configuration** sections of the page, select and type the attributes you want to edit for all selected APs.

NOTE

Only settings and options supported by all of the currently selected hardware types are available for configuring.

6 To save your changes, click **Save.**

Performing Altitude AP software maintenance

Periodically, the software used by the Altitude APs is altered for reasons of upgrade or security. The new version of the AP software is installed from the Summit WM Controller.

The software for each Altitude AP can be uploaded either immediately, or the next time the Altitude AP connects. Part of the Altitude AP boot sequence is to seek and install its software from the Summit WM Controller.

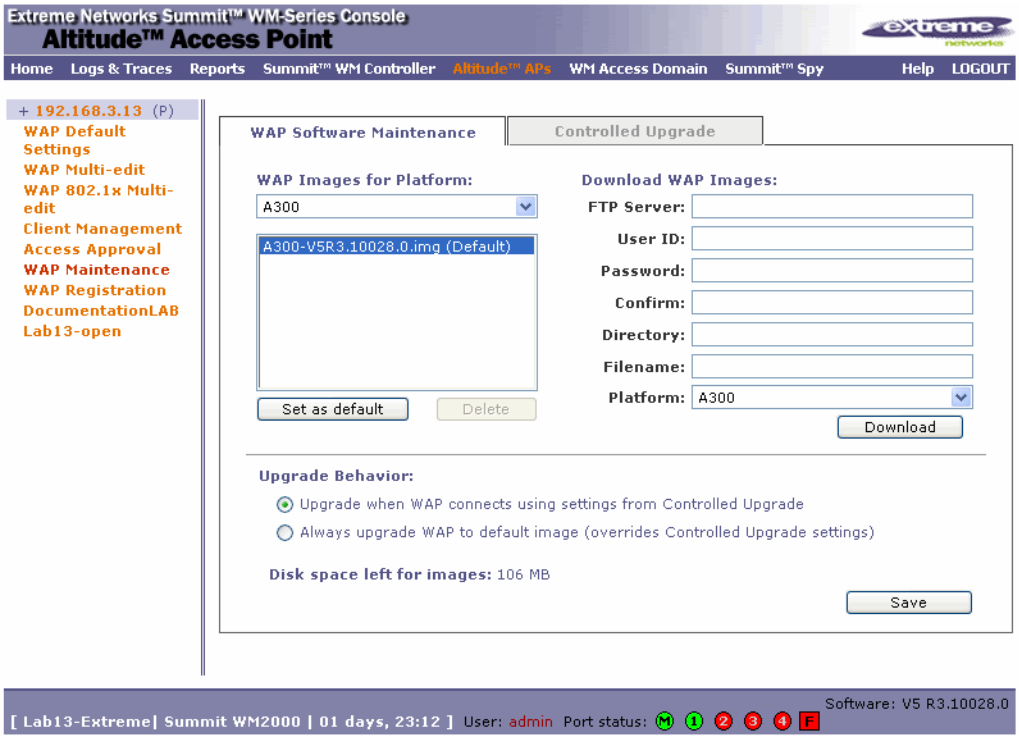
Most of the properties of each radio on an Altitude AP can be modified without requiring a reboot of the AP:

The Altitude AP keeps a backup copy of its software image. When a software upgrade is sent to the Altitude AP, the upgrade becomes the Altitude AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Altitude AP will run the backup image.

To maintain the list of current Altitude AP software images:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Maintenance** tab is displayed.



3 In the **WAP Images for Platform** drop-down list, click the appropriate platform.

4 To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.

5 In the **Upgrade Behavior** section, select one of the following:

- **Upgrade when AP connects using settings from Controlled Upgrade** - The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.
- **Always upgrade AP to default image (overrides Controlled Upgrade settings)** - Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.

6 To save your changes, click **Save**.

To delete an Altitude AP software image:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 In the **WAP Images for Platform** drop-down list, click the appropriate platform.

4 In the **WAP Images** list, click the image you want to delete.

5 Click **Delete**. The image is deleted.

To download a new Altitude AP software image:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 In the **Download WAP Images** list, type the following:

- **FTP Server** - The IP of the FTP server to retrieve the image file from.
- **User ID** - The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password** - The corresponding password for the user ID.
- **Confirm** - The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** - The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** - The name of the image file to retrieve.
- **Platform** - The AP hardware type to which the image applies. The are several types of AP and they require different images.

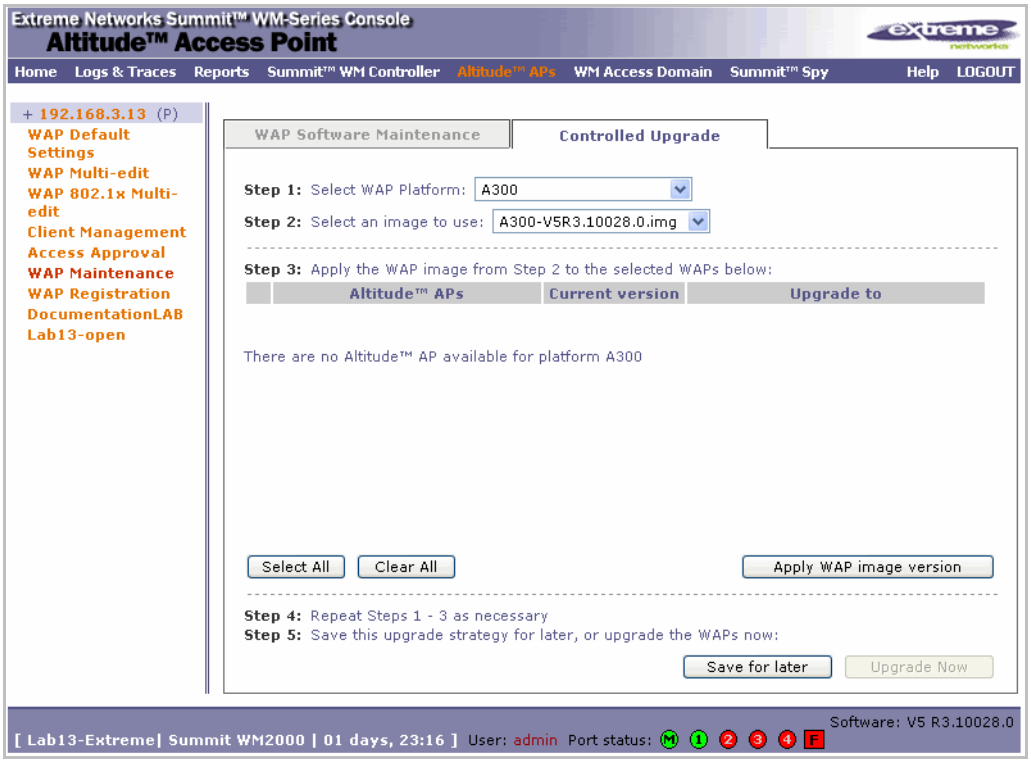
4 Click **Download**. The new software image is downloaded.

To define parameters for an Altitude AP controlled software upgrade:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 Click the **Controlled Upgrade** tab.



NOTE

*The **Controlled Upgrade** tab will appear only when the **Upgrade Behavior** is set to Upgrade when AP connects using settings from **Controlled Upgrade** on the **WAP Software Maintenance** tab.*

4 In the **Select WAP Platform** drop-down list, click the type of AP you want to upgrade.

5 In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.

6 In the list of registered **Altitude APs**, select the checkbox for each Altitude AP to be upgraded with the selected software image.

7 Click **Apply WAP image version**. The selected software image is displayed in the **Upgrade To** column of the list.

8 To save the software upgrade strategy to be run later, click **Save for later**.

9 To run the software upgrade immediately, click **Upgrade Now**. The selected Altitude AP reboots, and the new software version is loaded.

NOTE

*The **Always upgrade AP to default image** checkbox on the **WAP Software Maintenance** tab overrides the **Controlled Upgrade** settings.*

4 WM Access Domain Services

This chapter describes WM Access Domain Services (WM-AD) concepts, including:

- "WM-AD overview" on page 141
- "Setting up a WM-AD checklist" on page 142
- "Topology of a WM-AD" on page 143
- "RF assignment for a WM-AD" on page 145
- "Authentication for a WM-AD" on page 145
- "Filtering for a WM-AD" on page 146
- "Data protection on a WM-AD - WEP and WPA" on page 148
- "WM-AD global settings" on page 149
- "Setting up a new WM-AD" on page 153

WM-AD overview

A WM-AD is an IP subnet designed to enable Wireless APs to interact with wireless devices. A WM-AD is similar to a regular IP subnet. A WM-AD has the following properties:

- Each WM-AD is assigned a unique identifier.
- Each WM-AD is assigned a Service Set Identifier (SSID). The SSID does not have to be unique.
- Each WM-AD is assigned a range of IP addresses for wireless devices. All of the wireless devices share the same IP address prefix - the part of the IP address that identifies the network and subnet.

  NOTE

  If the WM-AD is in branch mode, the Summit WM Controller's DHCP server will not assign IP addresses to the wireless devices. For a routed WM-AD, you can allow the enterprise network's DHCP server to provide the IP addresses for the WM-AD by enabling DHCP Relay. The Summit WM Controller can also relay to an external DHCP server.
  The assigned addresses must be within range of the WM-AD definition and the controller must be defined in the network as the path for traffic delivery to the mobile units. For more information, see "Using a DHCP relay for the WM-AD" on page 162.

  These IP addresses are not virtual IP addresses. They are regular IP addresses and are unique over the network. These IP addresses are advertised to other hosts on the network to exchange traffic with the wireless devices in the WM-AD.
- A single overall filtering policy applies to all the wireless devices within the WM-AD. Additional filtering can be applied when the wireless user is authenticated by the Remote Authentication Dial-In User Service (RADIUS) server. This does not apply for a bridged WM-AD.
- When the Summit WM Controller creates a WM-AD, it also creates a virtual IP subnet for that WM-AD. This does not apply for a bridged WM-AD at the WAP. It does apply for **Bridge Traffic Locally as SWM**. In fact, the IP Address assigned to the interface of a Bridged at Summit WM WM-AD needs to be in the same subnet as the mobile units otherwise problems might occur.

- Each WM-AD represents a mobility group that, when configured, can be carried across multiple Summit WM Controllers. This does not apply for a bridged WM-AD at the WAP.
- Each WM-AD also offers unique Authentication, Authorization and Accounting (AAA) services.

Setting up a WM-AD checklist

WM-AD provides a versatile means of mapping wireless networks to the topology of an existing wired network. When you set up a WM-AD on the Summit WM Controller, you are defining a subnet for a group of wireless device users. The WM-AD definition creates a virtual IP subnet where the Summit WM Controller acts as a default gateway to wireless devices.

In addition you can determine if the WM-AD is to apply for traffic bridging at the AP. This type of WM-AD requires specification of RF parameters and authentication parameters (if AAA type), although filtering specifications and topology specifications do not apply.

The Summit WM Controller WM20/WM200/2000 provides the option to define a WM-AD as locally bridged to a VLAN at the controller. To support that configuration, you must define which VLAN the WM-AD should bridge to. With this configuration, it is possible that the controller is not involved in the IP address assignment for user addresses. Instead, the IP addresses for users are assigned directly by the DHCP infrastructure that services the VLAN.

NOTE

In a VLAN-bridged WM-AD, the default configuration dictates that the controller is not the DHCP server for that segment. However, DHCP services can selectively be enabled, including DHCP Relay, allowing you to use the controller to become the default DHCP server for the VLAN, if applicable.

Before defining a WM-AD, the following properties must be determined:

- A user access plan for both individual users and user groups
- The RADIUS attribute values that support the user access plan
- The location and identity of the Wireless APs that will be used on the WM-AD
- The routing mechanism to be used on the WM-AD
- For tunneled configurations mostly, the network addresses that the WM-AD will use
- A VLAN bridged WM-AD (at the controller) requires the specification of the IP address for the controller's own interface point (Port) on that VLAN. In addition, if the you elect to have the controller operate as the default DHCP server for the VLAN, the corresponding IP topology for that subnet must also be specified.
- The type of authentication for wireless device users on the WM-AD
- The specific filters to be applied to the defined users and user groups to control network access
- The quality of service (QoS) requirements
- What privacy mechanisms should be employed between the Wireless APs and the wireless devices
- Classification list for traffic priority. For example, whether the WM-AD is to be used for voice traffic and if voice traffic is to be given priority.
- Whether the WM-AD traffic is to be bridged directly to the network at the AP or tunneled to the controller for forwarding. Bridging at the AP is useful in branch office deployments in which APs must provide service even when the connection to the controller is unavailable.

User access plan

The user access plan should analyze the enterprise network and identify which users should have access to which areas of the network. What areas of the network should be separated? Which users can go out to the World Wide Web?

The Controller, Access Points, and WM software system relies on authenticating users via a RADIUS server (or other authentication server). To make use of this feature, an authentication server on the network is required. Make sure that the server's database of registered users, with login identification and passwords, is current.

In the case of certificate-based installations, you must ensure that the proper user certificate profiles are setup on the RADIUS server.

NOTE

*To deploy Controller, Access Points, and WM software without a RADIUS server (and without authentication of users on the network), click **SSID** for network assignment (on the **Topology** tab). On the **Authentication - Configure Captive Portal** page, select the **No Captive Portal** option. There will be no authentication of users, but the Controller, Access Points, and WM software is otherwise operational.*

The user access plan should also identify the user groups in your enterprise, and the business structure of the enterprise network, such as:

- Department (such as Engineering, Sales, Finance)
- Role (such as student, teacher, library user)
- Status (such as guest, administration, technician)

For each user group, you should set up a filter ID attribute in the RADIUS server, and then associate each user in the RADIUS server to at least one filter ID name. You can define specific filtering rules, by filter ID attribute, that will be applied to user groups to control network access. Filtering is applied by the controller. Filter ID assignments is a configuration option, and not a requirement to setup per user filter ID definitions. If a filter is not returned by the Access-Accept confirmation for a particular user, the controller uses the default filter profile for the WM-AD as the applicable filter set.

Topology of a WM-AD

Before you decide if a WM-AD will participate in a VLAN and configure a WM-AD, define the global settings that will apply to all WM-AD definitions. For example, global settings can include identifying the location of the RADIUS servers and enabling priority traffic handling for voice-over-internet traffic and dynamic authorization server support.

The type of network assignment determines all the other factors of the WM-AD. There are two options for network assignment:

- **SSID**:
  - Has Captive Portal authentication, or no authentication
  - Requires restricted filtering rules before authentication
  - Requires filtering rules for group filter IDs after authentication. A default filter applies if a more specific filter is not indicated by the RADIUS Access-Accept response.
  - Used for a WM-AD supporting wireless voice traffic (QoS)

  - Used for a WM-AD supporting third-party APs
  - Has WEP and WPA-PSK privacy
- **AAA**:
  - Has 802.1X authentication
  - Requires filtering rules for group filter IDs and default filter. A definition of group filter IDs is optional. If a filter is not specified or not returned by the Access-Accept response, the default filter group is applied.
  - Has WEP and WPA privacy
  - Summit WM Controller is involved in authenticating users. 802.1X packets for AAA assignment are forwarded by the Wireless AP to the Summit WM Controller through to the RADIUS server.

Traffic behavior types

There are 4 traffic types available when setting up your WM-AD:

- Tunneled to controller = **Routed**
- Bridged at AP = **Bridge Traffic Locally at WAP**
- Bridged to VLAN at controller (not available in WM100/1000) = **Bridge Traffic Locally as SWM**
- Wireless Distribution System = **WDS**

The Altitude APs are assigned to the WM-AD by radios. A Wireless AP radio is available for WM-AD assignment until it has been assigned to a maximum eight WM-ADs with the exception of WDS WM-AD that can handle maximum of seven WM-ADs. For more information, see "Wireless Distribution System" on page 212.

The Summit WM Controller can support the following:

- WM200/2000 - Up to 64 WM-ADs
- WM20 - Up to 8 WM-ADs
- WM1000 - Up to 50 WM-ADs
- WM100 - Up to 32 WM-ADs

Once a WM-AD definition is saved, the Summit WM Controller updates this information on the Wireless AP. The WM-AD broadcasts the updates during beacon transmission, unless the SSID beacon is suppressed on the **Topology** tab.

The **Altitude AP Configuration** page lists defined WM-ADs and which radio each has been assigned to.

On the **Topology** tab, define parameters for DHCP for IP address assignment. DHCP IP assignment is not applicable to Bridged at AP mode. DHCP assignment is disabled by default for Bridged to VLAN mode. However, you can enable DHCP server/relay functionality to have the controller service the IP addresses for the VLAN (and wireless users).

You can also configure this WM-AD for management traffic or for third-party APs. For more information, see Chapter 8, "Working with third-party APs".

RF assignment for a WM-AD

The second step in setting up a WM-AD is to configure the RF assignment for the WM-AD. From the **RF** tab you assign APs to a WM-AD and SSID definitions.

Authentication for a WM-AD

The third step in setting up a WM-AD is to configure the authentication mechanism for the WM-AD. The authentication mechanism depends on the network assignment. In addition, all WM-AD definitions can include authentication by Media Access Control (MAC) address. Authentication by MAC address provides a method of access control for a user as it associates with the AP based on the device's MAC address.

Authentication with SSID network assignment

If network assignment is SSID, there are two authentication options:

- **None** - This authentication method is the default for a new SSID assignment WM-AD. Authentication WM-AD, unless MAC-based authorization is used, the default filter is applied, not the non-authentication filter. For more information, see "Filtering for a WM-AD" on page 146.
- **Captive Portal** - This authentication method employs a Web redirection which directs a user's Web session to an authentication server. Typically, the user must provide their credentials (userID, password) to be authenticated. The Captive Portal redirection operation will redirect any Web page requests corresponding to targets which are not explicitly allowed by the non-authenticated filter. The user's Web page is redirected to a defined authentication Web server. You must ensure that the authentication Web server is explicitly listed as an allowed destination for traffic to be able to access it. After authentication, the client will be redirected to the originally requested Web page or a configured default redirection Web page.

  The Summit WM Controller supports two modes of Captive Portal authentication:

  - **Internal Captive Portal** - The controller's own Captive Portal authentication page (configured as an editable form) is used to request user credentials.
  - **External Captive Portal** - An entity outside of the Summit WM Controller is responsible for handling the user authentication process, presenting the credentials request forms and performing user authentication procedures. The controller is then informed of the authentication results via its Business Echosystem's interfaces.

  Four authentication types are supported for Captive Portal authentication:

  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Windows-specific version of CHAP (MS CHAP)
  - MS CHAP v2 (Windows-specific version of CHAP, version 2)

  For Captive Portal authentication, the RADIUS server must support the selected authentication type: PAP, CHAP (RFC2484), MS-CHAP (RFC2433), or MS-CHAPv2 (RFC2759).

Authentication with AAA (802.1X) network assignment

If network assignment is AAA with 802.1X authentication, the wireless device user requesting network access must first be authenticated. The wireless device's client utility must support 802.1X. The user's request for network access along with login identification or a user profile is forwarded by the Summit WM Controller to a RADIUS server. The Summit WM Controller, Access Points, and WM software system supports the following authentication types:

- **Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)** - Relies on client-side and server-side certificates to perform authentication. Can be used to dynamically generate a Pairwise Master Key for encryption.
- **Extensible Authentication Protocol with Tunneled Transport Layer Security (EAP-TTLS)** - Relies on mutual authentication of client and server through an encrypted tunnel. Unlike EAP-TLS, it requires only server-side certificates. The client uses PAP, CHAP, or MS-CHAPv2 for authentication.
- **Protected Extensible Authentication Protocol (PEAP)** - Is an authentication protocol similar to TTLS in its use of server side certificates for server authentication and privacy and its support for a variety of user authentication mechanisms.

For 802.1X, the RADIUS server must support RADIUS extensions (RFC2869).

Until the access-accept is received from the RADIUS server for a specific user, the user is kept in an unauthenticated state. 802.1X rules dictate no other packets other than EAP are allowed to traverse between the AP and the Summit WM Controller until authentication completes. Once authentication is completed (access-accept is received), the user's client is then allowed to proceed with IP services, which typically implies the request of an IP address via DHCP.

In addition, the definition of a specific filter ID is optional configuration. If a specific filter ID is not defined or returned by the access-accept operation, the Summit WM Controller assigns the WM-AD' default filter for authenticated users.

NOTE

The Summit WM Controller only assigns the device's IP after the client requests one.

Both Captive Portal and AAA (802.1X) authentication mechanisms in Controller, Access Points, and WM software rely on a RADIUS server on the enterprise network. You can identify and prioritize up to three RADIUS servers on the Summit WM Controller - in the event of a failover of the active RADIUS server, the Summit WM Controller will poll the other servers in the list for a response. Once an alternate RADIUS server is found, it becomes the active RADIUS server, until it either also fails, or the administrator redefines another.

Filtering for a WM-AD

The WM-AD capability provides a technique to apply policy, to allow different network access to different groups of users. This is accomplished by packet filtering.

After setting authentication, define the filtering rules for the filters that apply to your network and the WM-AD you are setting up. Several filter types are applied by the Summit WM Controller:

- **Exception filter** - Protect access to a system's own interfaces, including the WM-AD's own interface. WM-AD exception filters are applied to user traffic intended for the Summit WM Controller's own

interface point on the WM-AD. These filters are applied after the user's specific WM-AD state assigned filters.

- **Non-authenticated filter with filtering rules that apply before authentication** - Controls network access and to direct users to a Captive Portal Web page for login.
- **Group filters, by filter ID, for designated user groups** - Controls access to certain areas of the network, with values that match the values defined for the RADIUS filter ID attribute.
- **Default filter** - Controls access if there is no matching filter ID for a user.

Within each type of filter, define a sequence of filtering rules. The filtering rule sequence must be arranged in the order that you want them to take effect. Each rule is defined to allow or deny traffic in either direction:

- **In** - From a wireless device in to the network
- **Out** - From the network out to a wireless device

Final filter rule

The final rule in any filter should act as a catch-all for any traffic that did not match a filter. This final rule should either allow all or deny all traffic, depending on the requirements for network access. For example, the final rule in a non-authenticated filter for Captive Portal is typically deny all. A final allow all rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found.

A default rule of deny all is automatically created by the system for initial filter definitions. The administrator can change the action to allow all. However, a default filter rule cannot be removed. Since a default filter rule provides a catch-all default behavior for packet handling, all applicable user defined filter rules must be defined prior to this rule.

Each rule can be based on any one of the following:

- Destination IP address or any IP address within a specified range that is on the network subnet (as a wildcard)
- Destination ports, by number and range
- Protocols (UDP, TCP, etc.)

Filtering sequence

The filtering sequence depends on the type of authentication used:

- **No authentication (network assignment by SSID)**

  Only the default filter will apply. Specific network access can be defined.

- **Authentication by captive portal (network assignment by SSID)**

  The non-authenticated filter will apply before authentication. Specific network access can be defined. The filter should also include a rule to allow DNS requests and all users to get as far as the Captive Portal Web page where the user can enter login identification for authentication. When authentication is returned, the filter ID group filters are applied. If no filter ID matches are found, then the default filter is applied. The filter ID group is an optional behavior specification. If a filter ID is not returned, or an invalid one is returned, the default filter group is applied.

- **Authentication by AAA (802.1X)**

AAA assignment requires that user authentication is completed using the 802.1X/EAP protocol before a user is granted access to a network resource. Therefor, the enforcement of non-authenticated traffic rules is not applicable. When authentication is returned, then the filter ID group filters are applied. A WM-AD can have a subgoup with Login-LAT-Group ID that has its own filtering rules. The Login-LAT-Group indicates that a user session should be associated with a more specific WM-AD (a child WM-AD). The sub-WM-AD provides a different topology definition than the parent WM-AD, as well as having its own set of filter definitions. Filter IDs returned in association with a Login-LAT-Group definition are applied to the user, in relation to the sub-WM-AD indicated by the Login-LAT-Group specification. If no filter ID matches are found, then the default filter is applied.

The following is a high-level description of how a Summit WM Controller filters traffic:

Step One - The Summit WM Controller attempts to match each packet of a WM-AD to the filtering rules that apply to the wireless device user.

Step Two - If a filtering rule is matched, the operation to allow or deny is executed.

Step Three - The next packet is fetched for filtering.

Data protection on a WM-AD - WEP and WPA

On wireless and wired networks, data is protected by encryption techniques. The type of data protection that is available depends on the WM-AD assignment mode:

- **SSID** - Only WEP and WPA (1 or 2) -PSK privacy types are available
- **AAA** - WEP, Dynamic WEP, and WPA (1 or 2) privacy types are available

Data protection encryption techniques

NOTE

Regardless of the Altitude AP model or WM-AD type, a maximum of 112 simultaneous clients, per radio, are supported by all of the data protection encryption techniques listed below.

- **Wired Equivalent Privacy (WEP)** - WEP encrypts data sent between wireless nodes. Each node must use the same encryption key.
- **Wi-Fi Protected Access Privacy (WPA v.1 and v.2)** - Encryption is by Advanced Encryption Standard (AES) or by Temporal Key Integrity Protocol (TKIP). Two modes are available:
  - **Enterprise** - Specifies 802.1X authentication and requires an authentication server
  - **Pre-Shared Key (PSK)** - Relies on a shared secret. The PSK is a shared secret (pass-phrase) that must be entered in both the Wireless AP or router and the WPA clients.

NOTE

The Wireless 802.11n AP does not support WPA v.1 and v.2 encryption. For more information, see "Configuring privacy for a WM-AD" on page 193.

WM-AD global settings

Before defining a specific WM-AD, define the global settings that will apply to all WM-AD definitions. These global settings include:

- Configuring the location and password of RADIUS servers on the enterprise network. The defined servers appear as available choices when you set up the authentication mechanism for each WM-AD.
- Defining the shared secret used to encrypt the Pairwise Master Key (PMK) for WPA2 v.2 pre-authentication between Summit WM Controllers on the network.
- Enabling Dynamic Authorization Server (DAS) configuration support.

NOTE

You should enable Dynamic Authorization Server (DAS) only if you have DAS Server deployed on your network.

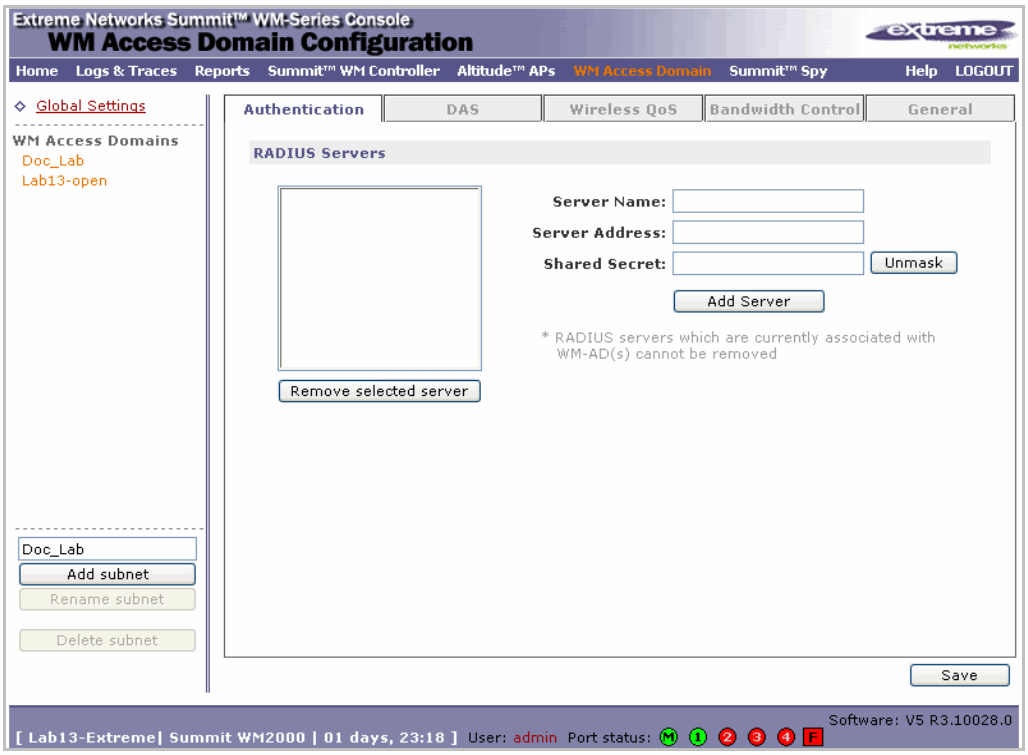
- Adjusting admission control thresholds. Admission control thresholds protect admitted traffic against overloads, provides distinct thresholds for VO and VI, and distinct thresholds for roaming and new streams.
- Defining Bandwidth Control Profiles. The Bandwidth Control Profiles you define appear as available choices in Bandwidth Control Profiles menu when you set up QoS policy for WM-ADs.

Defining RADIUS servers for Global Settings

To define RADIUS servers for WM-AD global settings:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.

2 In the left pane, click **Global Settings**. The **Authentication** tab is displayed.



3 To define a RADIUS server available on the network, do the following:

- In the **Server Name** box, type a name.
- In the **Server Address** box, type the IP address of the RADIUS server.
- In the **Shared Secret** box, type the password that is required in both directions. This password is used to validate the connection between controller and the RADIUS server.

4 In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.

This precautionary step is highly recommended in order to avoid an error, later, when the Summit WM Controller attempts to communicate with the RADIUS server.

5 To add the server to the list, click **Add**.

6 To remove a server, click the server in the list, and then click **Remove selected server**.

7 To save your changes, click **Save**.

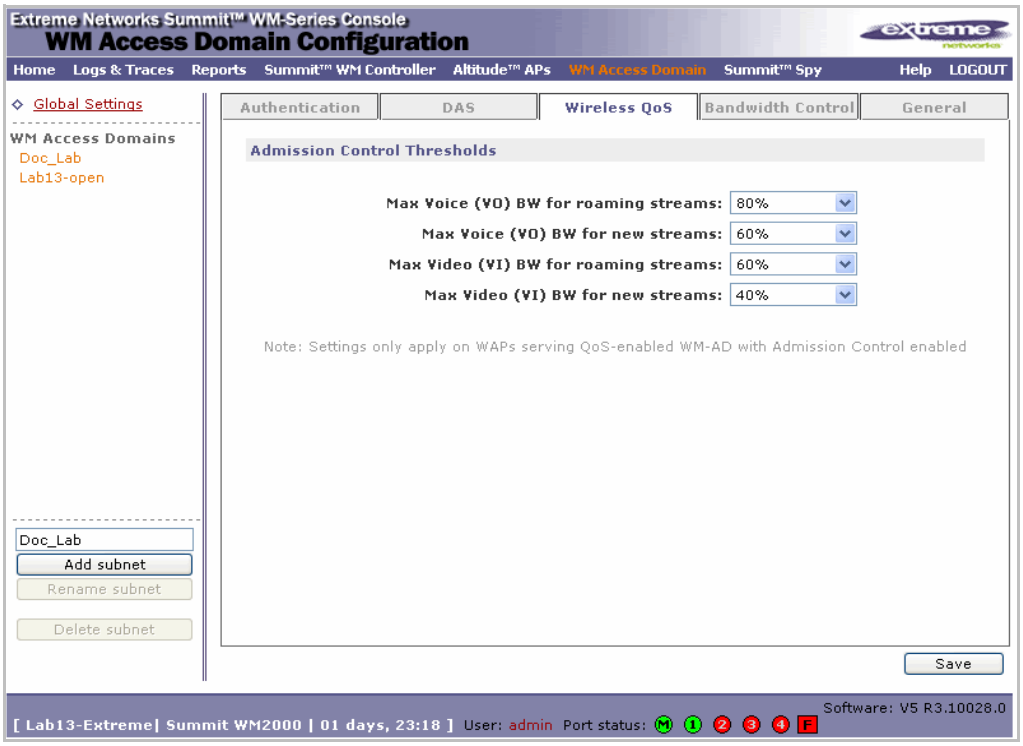
Defining Admission Control Thresholds for Global Settings

To define admission control thresholds for WM-AD global settings:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.

2 In the left pane, click **Global Settings**. The **Authentication** tab is displayed.

3 Click the **Wireless QoS** tab.



4 Using the percentage drop-down lists, define the thresholds for the following:

- **Max Voice (VO) BW for roaming streams** - The maximum allowed overall bandwidth on the new AP when a client with an active voice stream roams to a new AP and requests admission for the voice stream.
- **Max Voice (VO) BW for new streams** - The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new voice stream.
- **Max Video (VI) BW for roaming streams** - The maximum allowed overall bandwidth on the new AP when a client with an active video stream roams to a new AP and requests admission for the video stream.
- **Max Video (VI) BW for new streams** - The maximum allowed overall bandwidth on an AP when an already associated client requests admission for a new video stream.

These global QoS settings apply to all APs that serve QoS enabled WM-ADs with admission control.

5 To save your changes, click **Save**.

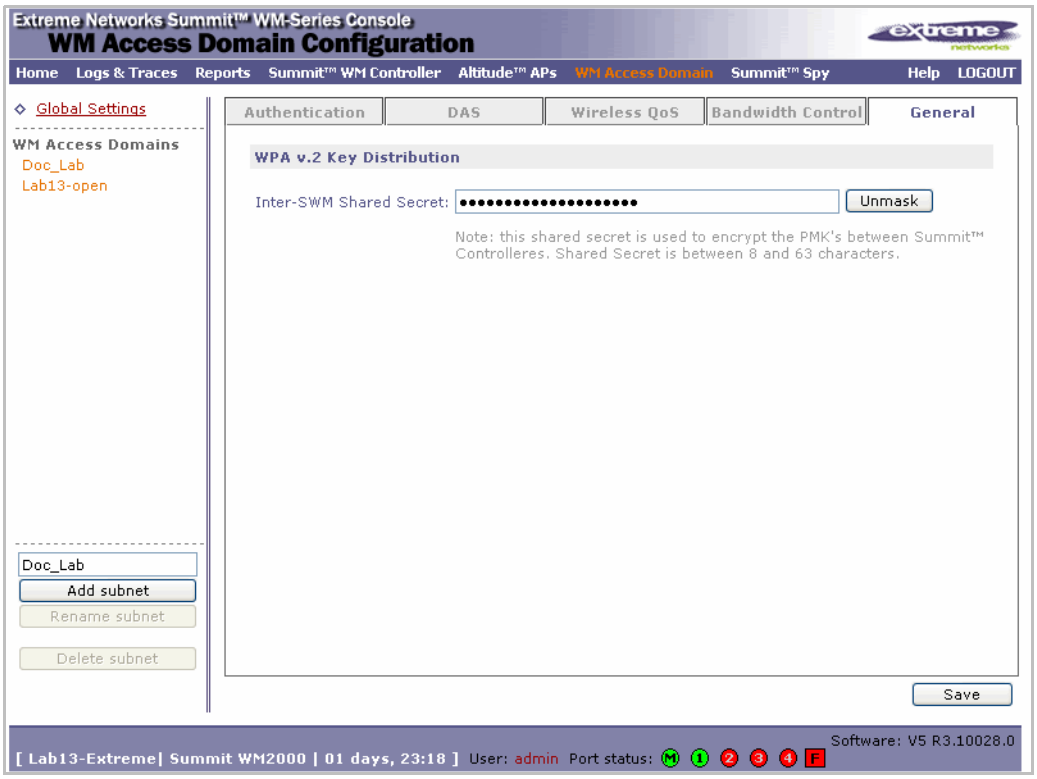
Defining inter-Summit WM Wireless Controller shared secret for Global Settings

To define inter-Summit WM Controller shared secret for WM-AD global settings:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domains** list is displayed.

2 In the left pane, click **Global Settings**.

3 Click the **General** tab.



4 In the **Inter-SWM Shared Secret** box, type a password between 8 and 63 characters long, to be used between Summit WM Controllers. The shared secret is to encrypt pre-shared keys that have to be moved between controllers for mobility. The same shared secret must also be defined on the other Summit WM Controllers on the network.

5 In order to proofread your password before saving the configuration, click **Unmask**. The password is displayed. To mask the password, click **Mask**.

This precautionary step is highly recommended in order to avoid an error, later, when the Summit WM Controller attempts to communicate with the RADIUS server.

6 To save your changes, click **Save**.

Creating Bandwidth Control profiles

The Bandwidth Control Profiles ensure that no single user on any WM-AD is able to consume disproportionate amount of bandwidth. A Bandwidth Control Profile consists of the following parameters:

- **Profile Name** - Name assigned to a profile
- **Committed Information Rate (CIR)** - Rate at which the network supports data transfer under normal operations. It is measured in kilobytes per second (Kbps).
- **Committed Burst Size (CBS)** - Number of bits that the Summit WM Controller can transmit over the WM-AD when congestion is occurring.

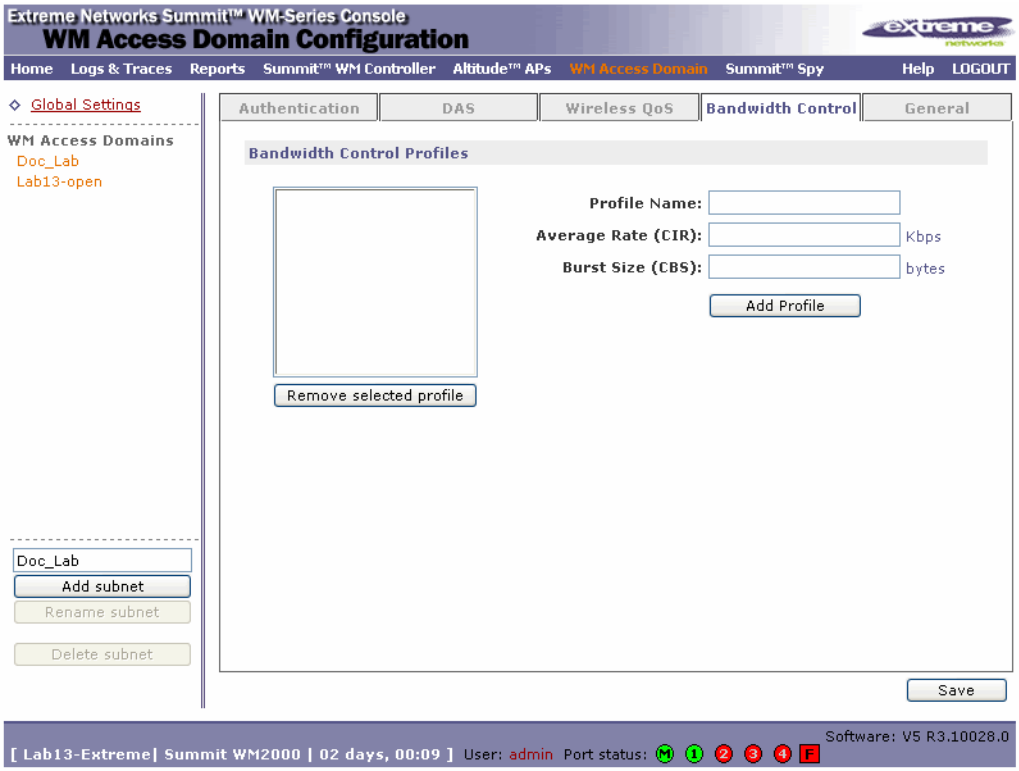
The Bandwidth Control Profiles you define on the WM-AD **Global Settings** screen appear as available choices in **Bandwidth Control Profiles** menu on the WM-AD **QoS Policy** screen.

To create a Bandwidth Control profile:

1 From the main menu, click **WM Access Domains**. The **WM-AD** list is displayed.

2 In the left pane, click **Global Settings**.

3 Click the **Bandwidth Control** tab.



4 Create a Bandwidth Control profile by doing the following:

- In the **Profile Name** box, type a name.
- In the **Average Rate (CIR)** box, type the CIR value.
- In the **Burst Size (CBS)** box, type the CBS value.

5 Click on **Add Profile**. The profile is created and the profile's name is displayed under the **Bandwidth Control Profiles** section.

NOTE

You can create as many profiles as you need.

6 To save your changes, click **Save**.

Setting up a new WM-AD

Now that you are familiar with the WM-AD concepts, you can now set up a new WM-AD. Setting up a new WM-AD involves the following general steps:

- Step one - Create a WM-AD name

- Step two - Define the topology parameters
- Step three - Configure the WM-AD

For information on setting up a new WM-AD, see Chapter 5, "WM Access Domain Services configuration."

5 WM Access Domain Services configuration

This chapter discusses WM-AD (WM Access Domain Services) configuration, including:

- "WM-AD Types" on page 156
- "Creating a new WM-AD name" on page 156
- "Topology for a WM-AD" on page 156
- "Assigning Altitude AP radios to a WM-AD" on page 164
- "Deleting a WM-AD" on page 166
- "Authentication for a WM-AD" on page 166
- "Defining accounting methods for a WM-AD" on page 179
- "Defining RADIUS filter policy for WM-ADs and WM-AD groups" on page 180
- "Configuring filtering rules for a WM-AD" on page 181
- "Enabling multicast for a WM-AD" on page 191
- "Configuring privacy for a WM-AD" on page 193
- "Defining a WM-AD with no authentication" on page 202
- "Defining priority level and service class for WM-AD traffic" on page 203
- "Working with Quality of Service (QoS)" on page 204
- "Configuring the QoS policy on a WM-AD" on page 206
- "Bridging traffic locally" on page 210
- "Wireless Distribution System" on page 212

Setting up a WM-AD defines a virtual IP subnet for a group of wireless device users, where the Summit WM Controller acts as a default gateway to wireless devices. For each WM-AD, you define its topology, authentication, accounting, RADIUS servers, filtering, multicast parameters, privacy and policy mechanism. When you set up a new WM-AD, additional tabs appear only after you save the topology.

NOTE

When configuring a WM-AD, you can navigate between the various WM-AD tabs and define your configuration without having to save your changes on each individual tab. Once your WM-AD configuration is complete, you can click Save on any WM-AD tab to save your complete WM-AD configuration.

NOTE

If you navigate away from the WM-AD tabs without saving your WM-AD changes, your WM-AD configuration changes will be lost.

WM-AD Types

The WM-AD topologies are classified on the basis of the following WM-AD types:

- **Routed WM-AD** - User traffic is tunneled to the Summit WM Controller. (This is the default setup.)
- **Bridged at the AP WM-AD** - User traffic is directly bridged to a VLAN at the AP network point of access (switch port).
- **VLAN bridged WM-AD** - User traffic is tunneled to the Summit WM Controller and is directly bridged at the controller to a specific VLAN. With this WM-AD type, mobile users become a natural extension of a VLAN subnet.
- **Wireless Distribution System** (**WDS**) - User traffic plies over a wireless network that uses multiple access points interconnected via wireless links. For more information, see "Deploying the WDS system" on page 220.

NOTE

The bridged at the controller, routed and bridged at the AP WM-ADs are the network WM-ADs and they are used to service the client devices. The WDS WM-AD is used for establishing WDS links between WDS Altitude APs.

Creating a new WM-AD name

Setting up a new WM-AD involves the following general steps:

- Step one - Create a WM-AD name:
- Step two - Defining the topology parameters
- Step three - Configuring the WM-AD

Before you can define the WM-AD topology parameters and configure the WM-AD, you must first create a new WM-AD name.

To create a new WM-AD name:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box.

3 Click **Add subnet**. The name is displayed in the **WM Access Domains** list. The **Topology** tab is displayed.

The following sections describe in detail how to define the WM-AD topology parameters and configure the WM-AD.

Topology for a WM-AD

On the **Topology** tab, the key choice for a WM-AD is the type of network assignment, which determines all the other factors of the WM-AD. When you have completed defining the topology for your WM-AD,

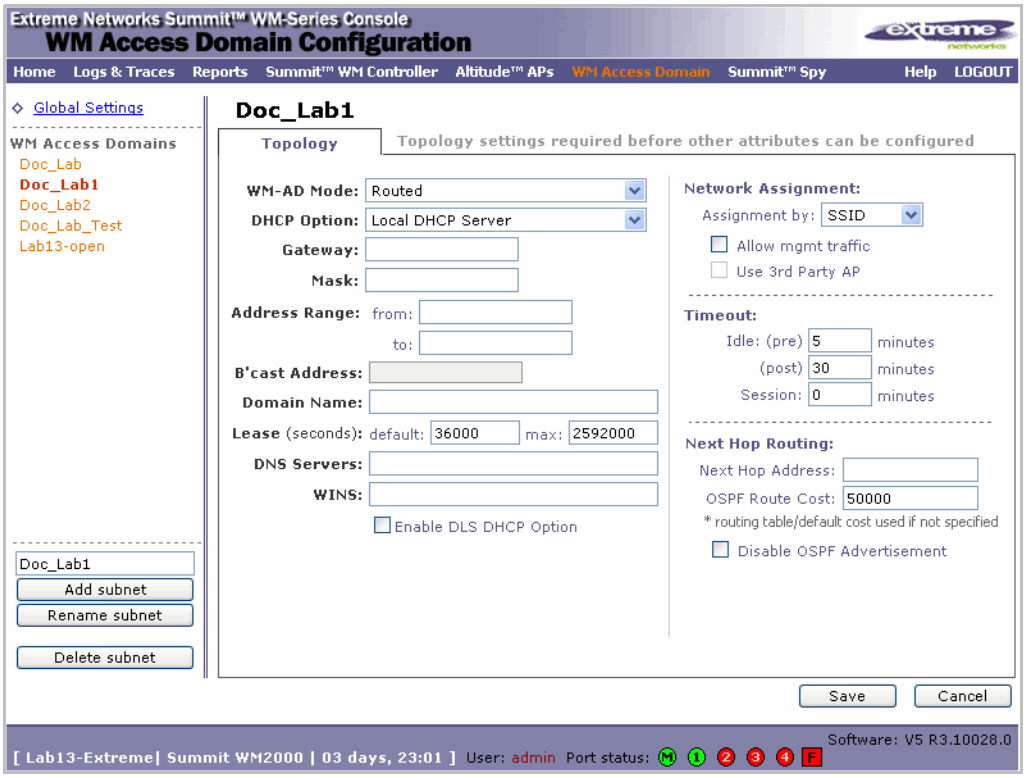
save the topology settings. Once your topology is saved, you can then access the remaining WM-AD tabs and continue configuring your WM-AD.

There are two options for network assignment:

- **SSID** - The SSID determines the WM-AD to which a user profile will be assigned (user topology/IP, filters):
  - Has Captive Portal authentication, or no authentication (as well as MAC-based authentication).
  - Requires restricted filtering rules before authentication and, after authentication, filtering rules for group filter IDs.
  - Is used for a WM-AD supporting wireless voice traffic (QoS).
  - Is used for a WM-AD supporting third-party APs.
  - Has WEP and WPA-PSK privacy.
- **AAA** (Authentication, Authorization and Accounting):
  - has 802.1X authentication (as well as MAC-based authentication).
  - requires filtering rules for group filter IDs and default filter.
  - has Dynamic WEP and WPA (WPA v.1 and WPA v.2) privacy.

Configuring topology for a WM-AD for Captive Portal

The section describes how to set up a WM-AD for Captive Portal. The **RF** tab, where you assign APs to WM-ADs, is not accessible until the topology for the WM-AD has been configured and saved.



To create an SSID for Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to create an SSID for. The **Topology** tab is displayed.

3 From the **Assignment by** drop-down list, click **SSID**.

Defining session timeout parameters

The Summit WM Controller allows a client to associate to the AP and exist on the network without having authentication. Every associated user has a user session tracked by the Summit WM Controller from the time of association with the AP. Users can be temporarily (or longer for SSID assigned WM-ADs) be in the non-authenticated state. Pre timeout is the maximum amount of time allowed to elapse from the last time any traffic was received by the system for an un-authenticated user. For example, a user may have disconnected from the system (shutdown the device, moved out of range, etc.). A pre timeout expires and cleans up the session.

The post timeout is the max amount of time that is allowed to elapse from the last time any traffic was received for an authenticated user. For example, a user may have disconnected from the system and is no longer be connected. A post timeout expires and cleans up the session.

A client that exceeds either the pre or post timeout value will be forced to disassociate.

The session timer defines the maximum amount of time a session is allowed to be connected to the system. The session timer is particularly useful in pay-per-use models. When the lifetime of the session reaches the defined limit, the session is expired and cleaned up. A user would have to re-authenticate with the system to continue to receive network services.

NOTE

The WM-AD timeout parameters define the default timers applicable to session management within the WM-AD. However, RADIUS authentication (access-accept) may return specific timers applicable to the particular user. A RADIUS returned value overwrites the WM-AD default values for the specific user.

In addition, a zero (0) value for any of the timers indicates a non-applicable value. Therefor, the corresponding timer is not enforced.

To define the session timeout parameters for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the session timeout parameters for. The **Topology** tab is displayed.

3 In the **Idle (pre)** box, type the number of minutes that a client is allowed to be idle on the WM-AD before authentication.

4 In the **Idle (post)** box, type the number of minutes that a client is allowed to be idle on the WM-AD after authentication.

5 In the **Session** box, type the maximum time limit of a session. If you do not provide a Session value, there is no time limit.

Enabling management traffic

If management traffic is enabled for a WM-AD, it overrides the built-in exception filters that prohibit traffic on the Summit WM Controller data interfaces. For more information, see "Configuring filtering rules for a WM-AD" on page 181.

To enable management traffic on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable management traffic for. The **Topology** tab is displayed.

3 Select the **Allow mgmt traffic** checkbox.

Enabling third-party APs on a WM-AD

Configuring a WM-AD for third-party APs is only available with SSID network assignment. Use this function as part of the process defined in Chapter 8, "Working with third-party APs."

A third-party AP WM-AD allows for the specification of a segregated subnet by which non-Altitude APs are used to provide RF services to users while still utilizing the Summit WM Controller for user authentication and user policy enforcement.

NOTE

Third-party AP devices are not fully integrated with the system and therefore must be managed individually to provide the correct user access characteristics. Also, third-party AP devices must be defined in bridge mode so that user traffic is directly transposed to the third-party AP subnet and picked up by the Summit WM Controller for forwarding and policy enforcement.

To enable third-party APs on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable third-party APs for. The **Topology** tab is displayed.

3 Select the **Use 3rd Party AP** checkbox.

The definition of third-party AP identification parameters allows the system to be able to differentiate the third-party AP device (and corresponding traffic) from user devices on that segment. Devices identified as third-party APs are considered pre-authenticated, and are not required to complete the corresponding authentication verification stages defined for users in that segment (typically Captive Portal enforcement).

In addition, third-party APs have a specific set of filters (third-party) applied to them by default, which allows the administrator to provide different traffic access restrictions to the third-party AP devices for the users that use those resources. The third-party filters could be used to allow access to third-party APs management operations (for example, HTTP, SNMP).

4 To save your changes, click **Save**.

Defining a next hop route and OSPF advertisement for a WM-AD

The next hop definition allows the administrator to define a specific host as the target for all non-WM-AD targeted traffic for users in a WM-AD. The next hop IP identifies the target device to which all WM-AD (user traffic) will be forwarded to. Next-hop definition supersedes any other possible definition in the routing table.

If the traffic destination from a wireless device on a WM-AD is outside of the WM-AD, it is forwarded to the next hop IP address, where this router applies policy and forwards the traffic. This feature applies to unicast traffic only. In addition, you can also modify the Open Shortest Path First (OSPF) route cost.

OSPF is an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately distributes the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place.

To define a next hop route and OSPF advertisement:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define a next-hop route for. The **Topology** tab is displayed.

3 In the **Next Hop Address** box, type the IP address of the next hop router on the network through which you wish all traffic on this WM-AD to be directed.

4 In the **OSPF Route Cost** box, type the OSPF cost of reaching the WM-AD subnet.

The OSPF cost value provides a relative cost indication to allow upstream routers to calculate whether or not to use the controller as a better fit or lowest cost path to reach devices in a particular network. The higher the cost, the less likely of the possibility that the controller will be chosen as a route for traffic, unless that controller is the only possible route for that traffic.

5 To disable OSPF advertisement on this WM-AD, select the **disable OSPF Advertisement** checkbox.

Defining the IP address for the WM-AD (for the DHCP server on the controller)

Bridged at the AP WM-ADs do not require the definition of a corresponding IP address definition for the WM-AD since all traffic for users in that WM-AD will be directly bridged by the AP at the local network point of attachment (VLAN at AP port).

The IP address definition is only required for a routed WM-AD or VLAN bridged WM-AD.

To define the IP address for the WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the IP address for. The **Topology** tab is displayed.

3 In the **Gateway** box, type the Summit WM Controller's own IP address in that WM-AD.

This IP address is the default gateway for the WM-AD. The Summit WM Controller advertises this address to the wireless devices when they sign on. For routed WM-ADs, it corresponds to the IP address that is communicated to MUs (in the WM-AD) as the default gateway for the WM-AD

subnet. (MUs target the Summit WM Controller's interface in their effort to route packets to an external host).

For a VLAN bridged WM-AD, the IP address corresponds to the Summit WM Controller's own point of presence on the VLAN. In this case, the controller's interface is typically not the gateway for the subnet. The gateway for the subnet is the infrastructure router defined to handle the VLAN.

NOTE

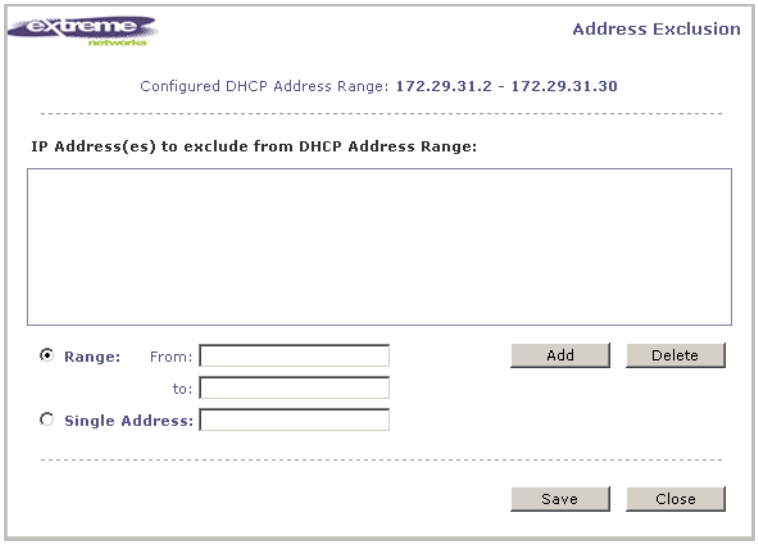
*If you are configuring Bridged at Controller WM-AD, the Gateway field appears as Interface **IP Addr** on the user interface.*

4 In the **Mask** box, type the appropriate subnet mask for this IP address to separate the network portion from the host portion of the address (typically 255.255.255.0).

The following values to DHCP configuration are only applicable for configurations if the controller is the DHCP server for users in the WM-AD - a routed WM-AD or a VLAN bridged WM-AD with DHCP enabled (by default, DHCP is disabled). These values are not visible for a bridged at AP WM-AD or a VLAN bridged WM-AD with DHCP disabled (by default, DHCP is disabled).

The **Address Range** boxes (from and to) populate automatically with the range of IP addresses to be assigned to wireless devices using this WM-AD, based on the IP address you provided.

- To modify the address in the **Address Range from** box, type the first available address.
- To modify the address in the **Address Range to** box, type the last available address.
- If there are specific IP addresses to be excluded from this range, click **Exclusion(s)**. The DHCP Address Exclusion window is displayed.



- In the DHCP Address Exclusion window, do one of the following:
  - To specify an IP range, type the first available address in the **From** box and type the last available address in the **to** box. Click **Add** for each IP range you provide.
  - To specify a IP address, select the **Single Address** option and type the IP address in the box. Click **Add** for each IP address you provide.
- To save your changes, click **Save**. The DHCP Address Exclusion window closes.

5 The **Broadcast Address** box populates automatically based on the Gateway IP address and subnet mask of the WM-AD.

6 In the **Domain Name** box, type the external enterprise domain name.

Modifying time limits for IP assignments

The following procedure is only applicable for configurations if the controller is the DHCP server for users in the WM-AD - a routed WM-AD or a VLAN bridged WM-AD with DHCP enabled (by default, DHCP is local). These values are not visible for a bridged at AP WM-AD or a VLAN bridged WM-AD with DHCP disabled (by default, DHCP is disabled).

Time limits for IP assignments dictate the default and the maximum time limits a wireless device can keep the DHCP server-assigned IP address.

To modify time limits for IP assignments:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to set time limits for. The **Topology** tab is displayed.
3. In the **Lease default** box, type the default time limit. The default time limit dictates how long a wireless device can keep the DHCP server assigned IP address. The default value is 36000 seconds (10 hours).
4. In the **Lease max** box, type the maximum time limit. The default time limit is 2539000 seconds (approximately 705 hours or 29 days).

Setting the name server configuration

Although this procedure could also apply to any WM-AD type, normally these settings are defined in the context of DHCP definitions and therefor these values are not available for configurations if DHCP service is not defined.

A VLAN bridged WM-AD has an option to define the DHCP behavior for the WM-AD. By default, the DHCP service is disable although the administrator can elect to have the controller's WM-AD interface on the VLAN become either the actual DHCP server (enable DHCP) or become the relay agent for DHCP requests.

To set the name server configuration:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.
2. In the left pane **WM Access Domains** list, click the WM-AD you want to set the name server configuration for. The **Topology** tab is displayed.
3. In the **DNS Servers** box, type the IP Address of the Domain Name Servers to be used.
4. If applicable, in the **WINS** box, type the IP address if the DHCP server uses Windows Internet Naming Service (WINS).

Using a DHCP relay for the WM-AD

Although this procedure could also apply to any WM-AD type, normally these settings are defined in the context of DHCP definitions and therefor these values are not available for configurations if DHCP service is not defined.

Using a DHCP relay forces the Summit WM Controller to forward DHCP requests to an external DHCP server on the enterprise network. This function bypasses the local DHCP server for the Summit WM Controller and allows the enterprise to manage IP address allocation to a WM-AD from its existing infrastructure.

The range of IP addresses assigned to the wireless device users on this WM-AD should also be designated on the external DHCP server.

To use an external DHCP server for the WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to use DHCP relay for. The **Topology** tab is displayed.

3 From the **DHCP Option** drop-down list, click **Use DHCP Relay**.

4 In the **Gateway** box, type the IP address for the WM-AD.

5 In the **Mask** box, type the appropriate subnet mask for this IP address.

6 In the **DHCP Server** box, type the IP address of the DHCP server to which DHCP discover and request messages will be forwarded for clients on this WM-AD. In the case of relay, the Summit WM Controller does not handle DHCP requests from users, but instead forwards the requests to the indicated DHCP server.

NOTE

The DHCP Server must be configured to match the WM-AD settings. In particular for Routed WM-AD', the DHCP server must identify the Summit WM Controller's interface IP as the default Gateway (router) for the subnet. (Users intending to reach devices outside of the subnet will forward the packets to the default gateway (controller) for delivery upstream.)

Configuring topology for a WM-AD for AAA

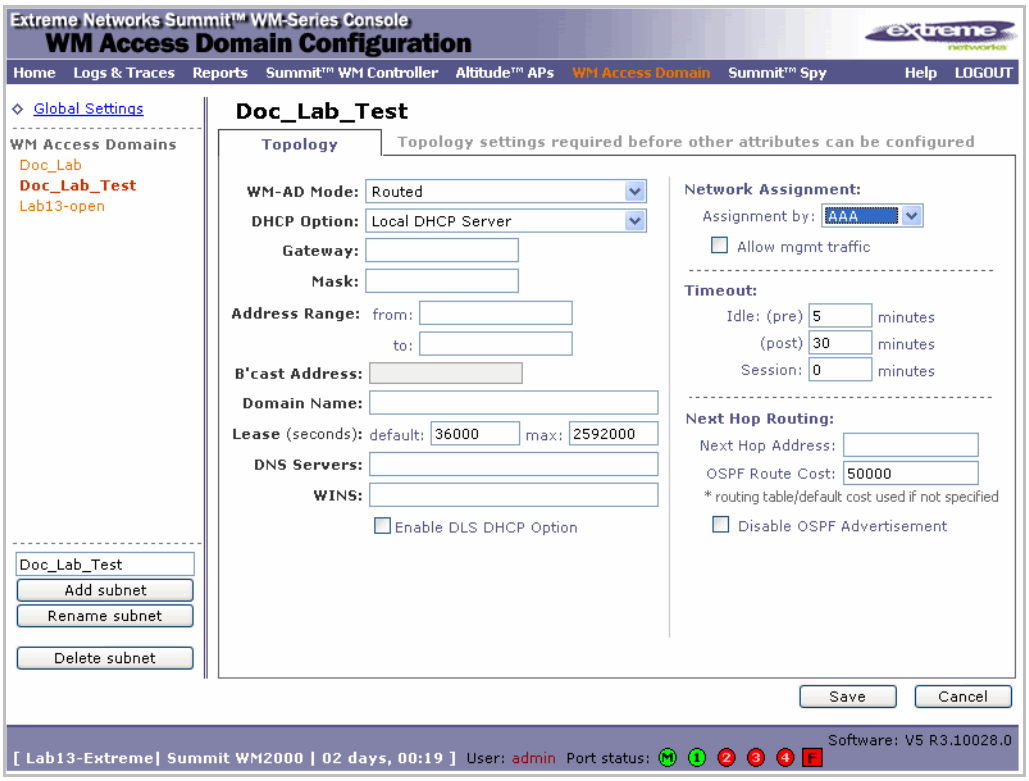
The following sections describe how to configure the topology for a WM-AD for AAA.

To create an AAA topology:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to create an AAA topology for. The **Topology** tab is displayed.

3 From the **Assignment by** drop-down list, click **AAA**.



4 Configure the topology for your WM-AD accordingly. For more information, see "Topology for a WM-AD" on page 156.

5 To save your changes, click **Save**.

Saving your topology properties

Once your topology is defined, you can then save your topology properties to continue configuring your WM-AD. To save your topology properties, click **Save**.

Assigning Altitude AP radios to a WM-AD

If two Summit WM Controllers have been paired for availability (for more information, see Chapter 6, "Availability and session availability"), each Summit WM Controller's registered Altitude APs will appear as foreign in the list of available Altitude APs on the other Summit WM Controller.

Once you have assigned an Altitude AP radio to eight WM-ADs, it will not appear in the list for another WM-AD setup. Each radio can support up to eight SSIDs (16 per AP). Each AP can be assigned to any of the WM-ADs defined within the system. The Summit WM Controller can support the following:

- WM200/2000 - Up to 64 WM-ADs
- WM20 - Up to 8 WM-ADs
- WM1000 - Up to 50 WM-ADs

- WM100 - Up to 32 WM-ADs

NOTE

You can assign the radios of all three Altitude AP variants - Altitude AP, Outdoor AP, and Altitude 802.11n AP - to any WM-AD.

To assign Altitude APs to a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to assign Altitude APs to. The **Topology** tab is displayed.

3 Click the **RF** tab.

4 In the **SSID** box, type the SSID that wireless devices will use to access the Altitude AP.

5 In the **Advanced RF Settings**, select the following:

- **Suppress SSID** - Select to prevent this SSID from appearing in the beacon message sent by the Altitude AP. The wireless device user seeking network access will not see this SSID as an available choice, and will need to specify it.
- **Enable proprietary IE** - Select to enable radio channel reports to be sent to the Altitude AP for improving roaming time and reliability, as well as improving client power consumption. The AP channel report lists all channels on which the WM-AD can be found - all channels used by all APs that have been assigned to the WM-AD. The AP will provide this list in a proprietary information element to be included in Beacon and Probe response packets. By default this option is disabled. It is recommended to enable this option.
- **Enable 11h support** - Select to enable TPC (Transmission Power Control) reports. By default this option is disabled. It is recommended to enable this option.
  - **Apply power back-off** - Select to enable the AP to use reduced power (as does the 11h client). By default this option is disabled. It is recommended to enable this option.
- **Process client IE requests** - Select to enable the AP to accept IE requests sent by clients via Probe Request frames and responds by including the requested IE's in the corresponding Probe Response frames. By default this option is disabled. It is recommended to enable this option.

6 From the **Altitude APs** list, click the APs and their radios that you want to assign to the WM-AD. You can also use the **Select APs** list, to select APs and their radios by grouping:

- **All radios** - Click to assign all of the APs' radios.
- **11a radios** - Click to assign only the APs' 11a radios.
- **11b/g radios** - Click to assign only the APs' 11b/g radios.
- **local APs - all radios** - Click to assign only the local APs.
- **local APs - 11a radios** - Click to assign only the local APs' 11a radios.
- **local APs - 11b/g radios** - Click to assign only the local APs' 11b/g radios.
- **foreign APs - all radios** - Click to assign only the foreign APs.
- **foreign APs - 11a radios** - Click to assign only the foreign APs' 11a radios.
- **foreign APs - 11b/g radios** - Click to assign only the foreign APs' 11b/g radios.
- **clear all selections** - Click to clear all of the AP radio assignments.
- **original selections** - Click to return to the AP radio selections prior to the most recent save.

7 To save your changes, click **Save**.

You can view the WM-ADs that each radio is assigned to by clicking the radio tabs from the **Altitude AP Configuration** page.

Deleting a WM-AD

You can delete the WM-ADs that are not in use.

To delete the WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 From the list of **WM Access Domains**, click the WM-AD.

3 To delete the WM-AD, click **Delete subnet**.

Authentication for a WM-AD

The next step in configuring a WM-AD is to set up the authentication mechanism. There are various authentication combinations available:

- If network assignment is by SSID, authentication can be:
  - none
  - by Captive Portal using internal Captive Portal
  - by Captive Portal using external Captive Portal
  - by MAC-based authentication
- If network assignment is by AAA (802.1X), authentication can be:
  - by 802.1X authentication, the wireless device user must be authenticated before gaining network access
  - by MAC-based authentication

The first step for any type of authentication is to select RADIUS servers for:

- Authentication
- Accounting
- MAC-based authentication

MAC-based authentication enables network access to be restricted to specific devices by MAC address. In addition to the other types of authentication, when MAC-based authentication is employed the Summit WM Controller queries a RADIUS server to determine if the wireless client's MAC address is authorized to access the network.

Vendor Specific Attributes

In addition to the standard RADIUS message, you can include Vendor Specific Attributes (VSAs). The Controller, Access Points and Convergence Software authentication mechanism provides six VSAs for RADIUS and other authentication mechanisms.

Table 14: Vendor Specific Attributes

Attribute Name	ID	Type	Messages	Description
Extreme-URL-Redirection	1	string	Returned from RADIUS server	A URL that can be returned to redirect a session to a specific Web page.
Extreme-AP-Name	2	string	Sent to RADIUS server	The name of the AP the client is associating to. It can be used to assign policy based on AP name or location.
Extreme-AP-Serial	3	string	Sent to RADIUS server	The AP serial number. It can be used instead of (or in addition to) the AP name.
Extreme-WM-AD-Name	4	string	Sent to RADIUS server	The name of the WM Access Domain the client has been assigned to. It is used in assigning policy and billing options, based on service selection.
Extreme-SSID	5	string	Sent to RADIUS server	The name of the SSID the client is associating to. It is used in assigning policy and billing options, based on service selection.
Extreme-BSS-MAC	6	string	Sent to RADIUS server	The name of the BSS-ID the client is associating to. It is used in assigning policy and billing options, based on service selection and location.

The first five of these VSAs provide information on the identity of the specific Altitude AP that is handling the wireless device, enabling the provision of location-based services.

The RADIUS message also includes RADIUS attributes Called-Station-Id and Calling-Station-Id in order to include the MAC address of the wireless device.

NOTE

Extreme-URL-Redirection is supported by MAC-based authentication.

Defining authentication for a WM-AD for Captive Portal

For Captive Portal authentication, the wireless device connects to the network, but can only access the specific network destinations defined in the non-authenticated filter. For more information, see "Defining non-authenticated filters" on page 183. One of these destinations should be a server, either internal or external, which presents a Web login page - the Captive Portal. The wireless device user must input an ID and a password. This request for authentication is sent by the Summit WM Controller to a RADIUS server or other authentication server. Based on the permissions returned from the authentication server, the Summit WM Controller implements policy and allows the appropriate network access.

Captive Portal authentication relies on a RADIUS server on the enterprise network. There are three mechanisms by which Captive Portal authentication can be carried out:

- **Internal Captive Portal** - The Summit WM Controller displays the Captive Portal Web page, carries out the authentication, and implements policy.
- **External Captive Portal** - After an external server displays the Captive Portal Web page and carries out the authentication, the Summit WM Controller implements policy.
- **External Captive Portal with internal authentication** - After an external server displays the Captive Portal Web page, the Summit WM Controller carries out the authentication and implements policy.

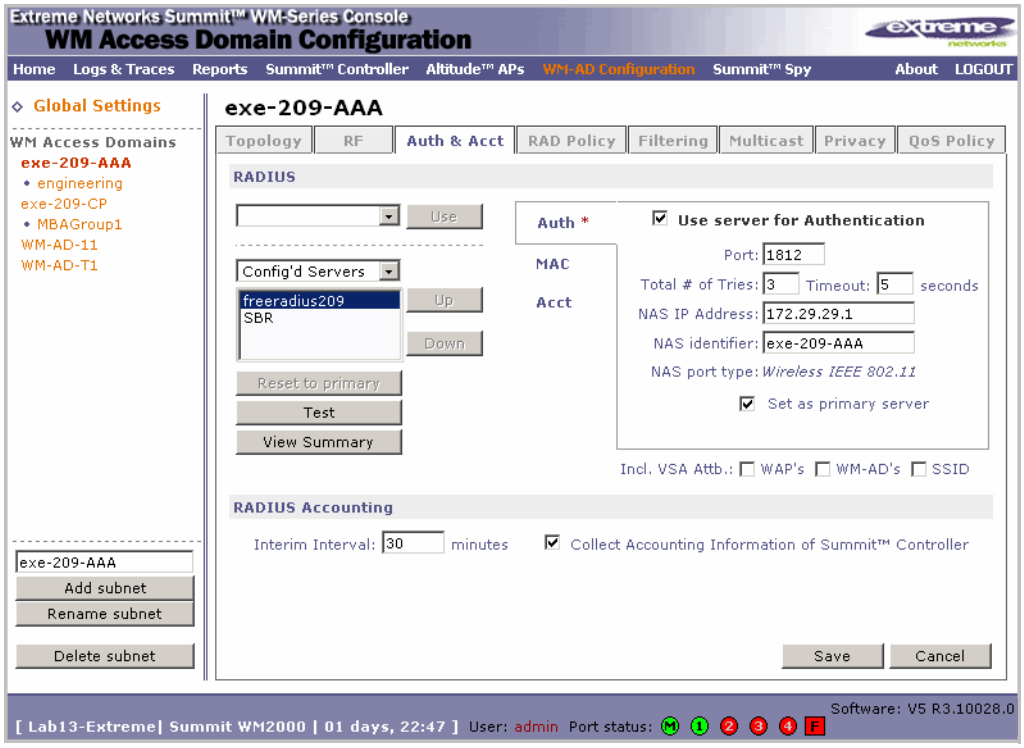
To define authentication by Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up authentication by Captive Portal for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

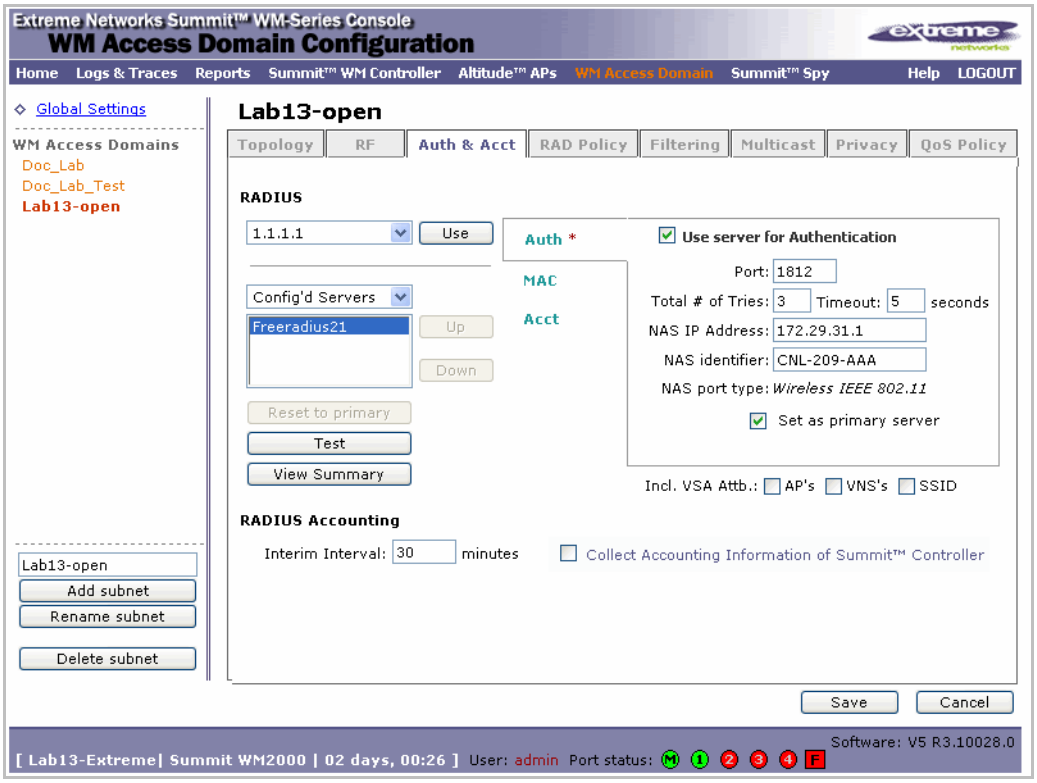
- **Auth** - Use to define authentication servers.
- **MAC** - Use to define servers for MAC-based authentication.
- **Acct** - Use to define accounting servers.



4 Click **Auth**. The Authentication fields are displayed.

5 From the **RADIUS** drop-down list, click the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

The RADIUS servers are defined on the **Global Settings** page. For more information, see "WM-AD global settings" on page 149.



The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

7 In the **# of Retries** box, type the number of times the Summit WM Controller will attempt to access the RADIUS server.

8 In the **Timeout** box, type the maximum time that a Summit WM Controller will wait for a response from the RADIUS server before attempting again.

9 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

10 In the **Auth. Type** drop-down list, click the authentication protocol to be used by the RADIUS server to authenticate the wireless device users. The authentication protocol applies to a WM-AD with Captive Portal authentication:

- **PAP** - Password Authentication Protocol
- **CHAP** - Challenge Handshake Authentication Protocol
- **MS-CHAP** - Windows-specific version of CHAP
- **MS-CHAP2** - Windows-specific version of CHAP, version 2

11 In the **Include VSA Attributes** section, click the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- **WM-AD's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

12 If appropriate, select the **Reset to Primary** checkbox. This checkbox is visible when a RADIUS server has not yet been selected as a primary server, or if the server you are configuring has already been selected as the primary server, the **Reset to Primary** checkbox is selected.

RADIUS redundancy defines additional backup RADIUS servers that the system will attempt to communicate with in case a connection with the identified primary server fails. If connection to an active primary server fails, the system automatically attempts to connect to one of the alternate servers in sequence. If the system succeeds in registering with a defined alternate server, it becomes the active primary server, which is identified by the A on the list. You can subsequently reset or change the identification of the primary server by selecting the applicable **Reset to Primary** checkbox.

13 To save your changes, click **Save**.

NOTE

*If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the **Up** and **Down** buttons and select the **Use server for Authentication** checkbox. The server's default information is displayed.*

Defining the RADIUS server priority for RADIUS redundancy

If more than one server has been defined for any type of authentication, you can define the priority of the servers in the case of failover.

In the event of a failover of the main RADIUS server - if there is no response after the set number of retries - then the other servers in the list will be polled on a round-robin basis until a server responds.

If one of the other servers becomes the active server during a failover, when the new active server properties are displayed the **Set as primary server** checkbox is selected.

If all defined RADIUS servers fail to respond, a critical message is generated in the logs.

To define the RADIUS server priority for RADIUS redundancy:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the RADIUS server priority for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 From the drop-down list, click the servers group you want to prioritize:

- Configured Servers
- Authentication Servers
- MAC Servers

- Accounting Servers

5 In the server list, click the RADIUS server and then click **Up** or **Down** to arrange the order. The first server in the list is the active one.

6 To test the Summit WM Controller's connection to all configured RADIUS servers, click **Test**. The Test RADIUS servers page displays the message transaction with the RADIUS server, which allows you to visually verify the state of the server connection and user authentication.

   The RADIUS test is a test of connectivity to the RADIUS server, not of full RADIUS functionality. AAA WM-ADs use EAP over RADIUS for authentication. The Summit WM Controller's EAP RADIUS connectivity test initiates an Access-Request, to which the RADIUS server will respond with a challenge. If the challenge is received then the test is deemed to have succeeded. If the challenge is not received then the test is deemed to have failed. In either case, the test ends at this point; for AAA WM-ADs, there is no need for a client password below.

7 In the **User ID** box, type the user ID that you know can be authenticated.

8 In the **Password** box, type the corresponding password.

9 Click **Test**. The **Test Result** page is displayed.

10 To view a summary of the RADIUS configuration, click **View Summary**. The **RADIUS summary** page is displayed.

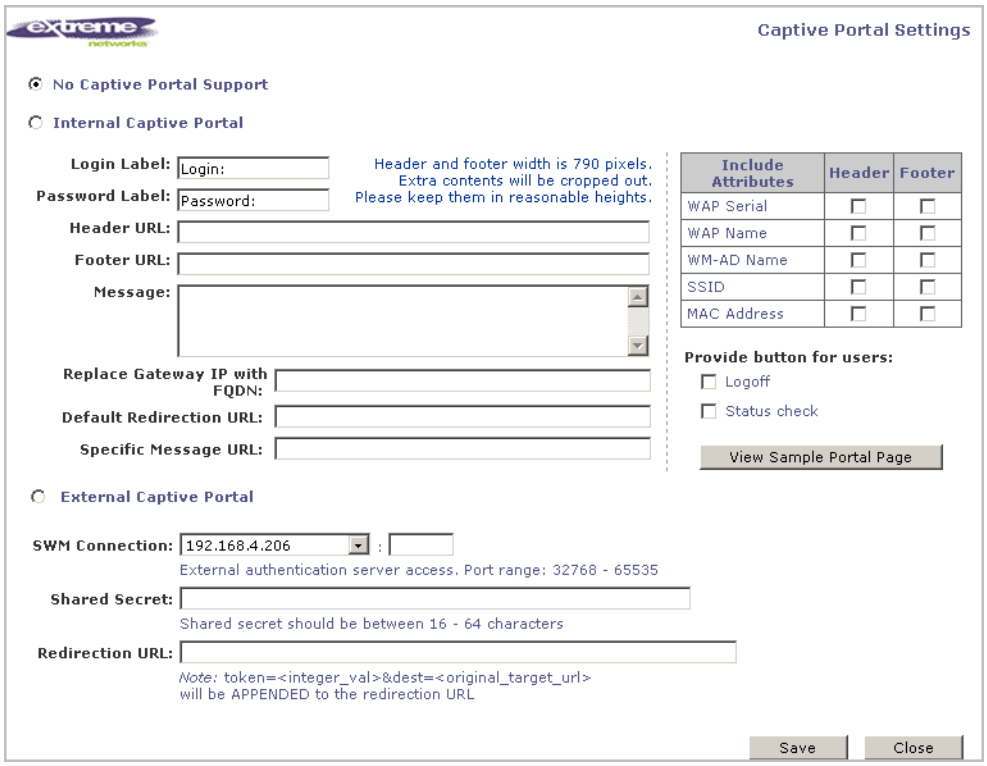
11 To save your changes, click **Save**.

Configuring Captive Portal for internal or external authentication

There are three Captive Portal options:

- **No Captive Portal Support**
- **Internal Captive Portal** - Define the parameters of the internal Captive Portal page displayed by the Summit WM Controller, and the authentication request from the Summit WM Controller to the RADIUS server.
- **External Captive Portal** - Define the parameters of the external Captive Portal page displayed by an external server. The authentication can be carried out by an external authentication server or by the Summit WM Controller request to a RADIUS server.

For more information, see "To configure the Captive Portal settings for internal Captive Portal:" on page 172 or "To configure the Captive Portal Settings for external Captive Portal:" on page 173.



To configure the Captive Portal settings for internal Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure the Captive Portal settings for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** page is displayed.

5 Select the **Internal Captive Portal** option.

6 In the **Login Label** box, type the text that will appear as a label for the user login field.

7 In the **Password Label** box, type the text that will appear as a label for the user password field.

8 In the **Header URL** box, type the location of the file to be displayed in the Header portion of the Captive Portal page. This page can be customized to suit your organization, with logos or other graphics.

CAUTION

If you use logos or graphics, ensure that the graphics or logos are appropriately sized. Large graphics or logos may force the login section out of view.

9 In the **Footer URL** box, type the location of the file to be displayed in the Footer portion of the Captive Portal page.

10 In the **Message** box, type the message that will appear above the Login box to greet the user. For example, the message could explain why the Captive Portal page is appearing, and instructions for the user.

11 In the **Replace Gateway IP with FQDN** box, type the appropriate name if a Fully Qualified Domain Name (FQDN) is used as the gateway address.

12 In the **Default Redirection URL** box, type the URL to which the wireless device user will be directed to after authentication.

13 In the **Specific Message URL** box, type the URL of a document that will be displayed in a text frame on the Captive Portal login page. This text frame can be used to display lengthier messages, such as terms and conditions of use for users who have not yet logged in.

14 In the right pane, select the appropriate checkboxes to include the following VSA Attributes in the message to the authentication server:

- AP Serial number
- AP Name
- WM-AD Name
- SSID
- MAC Address

15 In the right pane, select whether these VSA attributes apply to the header or footer of the Captive Portal page.

The selections influence what URL is returned in either section. For example, wireless users can be identified by which Altitude AP or which WM-AD they are associated with, and can be presented with a Captive Portal Web page that is customized for those identifiers.

16 To provide users with a logoff button, select **Logoff**. The Logoff button launches a pop-up logoff page, allowing users to control their logoff.

17 To provide users with a status check button, select **Status check**. The Status check button launches a pop-up window, which allows users to monitor session statistics such as system usage and time left in a session.

18 To save your changes, click **Save**.

19 To see how the Captive Portal page you have designed will look, click **View Sample Portal Page**.

CAUTION

In order for Captive Portal authentication to be successful, all the URLs referenced in the Captive Portal setup must also be specifically identified and allowed in the non-authenticated filter. For more information, see *"Defining non-authenticated filters" on page 183*.

To configure the Captive Portal Settings for external Captive Portal:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure the Captive Portal settings for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** page is displayed.

5 Select the **External Captive Portal** option.

6 In the **WM Connection** drop-down list, click the IP address.

7 Type the port of the Summit WM Controller.

If there is an authentication server configured for this WM-AD, the external Captive Portal page on the external authentication server will send the request back to the Summit WM Controller to allow the Summit WM Controller to continue with the RADIUS authentication and filtering.

In the **Shared Secret** box, type the password common to both the Summit WM Controller and the external Web server if you want to encrypt the information passed between the Summit WM Controller and the external Web server.

8 In the **Redirection URL** box, type the URL to which the wireless device user will be directed to after authentication.

9 To save your changes, click **Save**.

NOTE

You must add a filtering rule to the non-authenticated filter that allows access to the External Captive Portal site. For more information, see "Filtering for a WM-AD" on page 146.

Defining authentication for a WM-AD for AAA

If network assignment is AAA with 802.1X authentication, the wireless device must successfully complete the user authentication verification prior to being granted network access. This enforcement is performed by both the user's client and the AP. The wireless device's client utility must support 802.1X. The user's EAP packets request for network access along with login identification or a user profile is forwarded by the Summit WM Controller to a RADIUS server.

NOTE

In order to use WPA with 802.1X authentication, network assignment must be AAA.

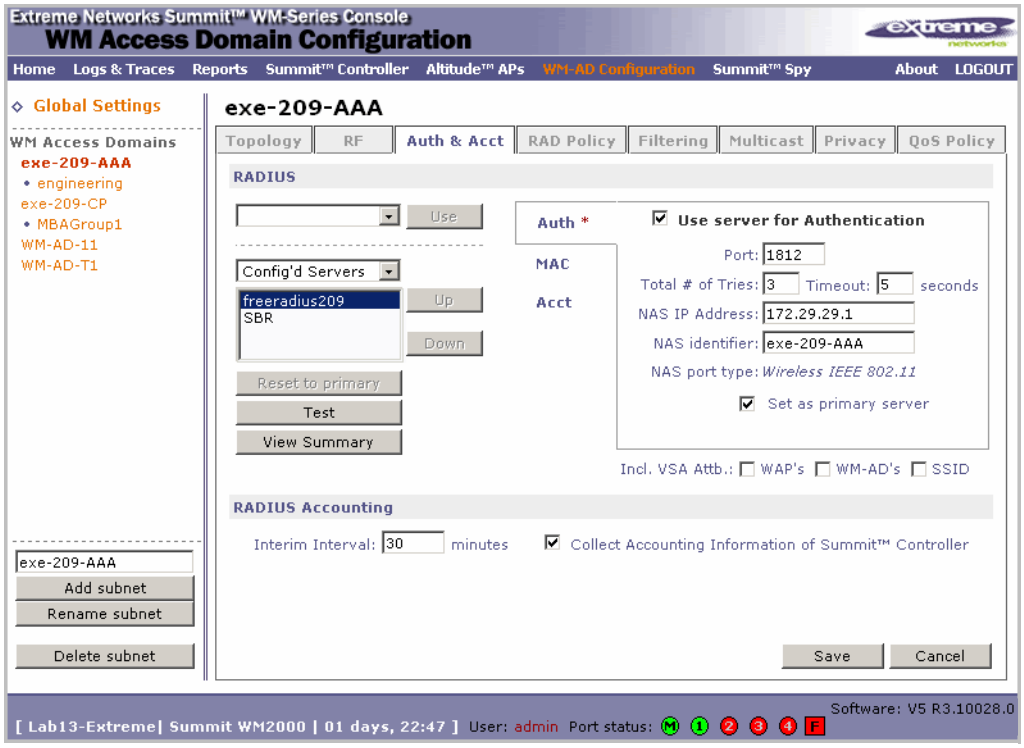
To define authentication by AAA (802.1X):

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up authentication by AAA for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

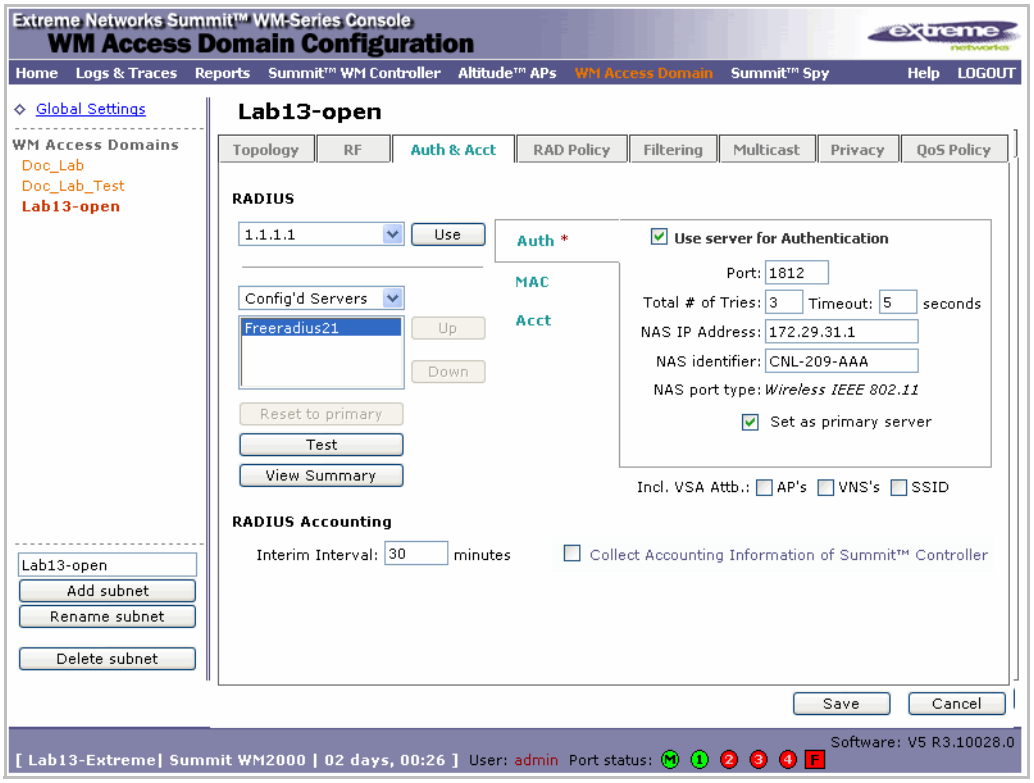
- **Auth** - Use to define authentication servers.
- **MAC** - Use to define servers for MAC-based authentication.
- **Acct** - Use to define accounting servers.



4 Click **Auth**. The Authentication fields are displayed.

5 From the **RADIUS** drop-down list, click the server you want to use for Captive Portal authentication, and then click **Use**. The server's default information is displayed.

The RADIUS servers are defined on the **Global Settings** page. For more information, see "WM-AD global settings" on page 149.



The selected server is no longer available in the **RADIUS** drop-down list.

The server name is now displayed in the list of configured servers, next to the **Up** and **Down** buttons, where it can be prioritized for RADIUS redundancy. The server can also be assigned again for MAC-based authentication or accounting purposes.

A red asterisk is displayed next to **Auth**, indicating that a server has been assigned.

6 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

7 In the **# of Retries** box, type the number of times the Summit WM Controller will attempt to access the RADIUS server.

8 In the **Timeout** box, type the maximum time that a Summit WM Controller will wait for a response from the RADIUS server before attempting again.

9 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

10 In the **Include VSA Attributes** section, select the appropriate checkboxes to include the Vendor Specific Attributes in the message to the RADIUS server:

- **AP's**
- **WM-AD's**
- **SSID**

The Vendor Specific Attributes must be defined on the RADIUS server.

11 If applicable, select the **Set as primary server** checkbox.

12 To save your changes, click **Save**.

NOTE

*If you have already assigned a server to either MAC-based authentication or accounting, and you want to use it again for authentication, highlight its name in the list next to the **Up** and **Down** buttons and select the **Use server for Authentication** checkbox. The server's default information is displayed.*

Defining MAC-based authentication for a WM-AD

MAC-based authentication enables network access to be restricted to specific devices by MAC address. The Summit WM Controller queries a RADIUS server for a MAC address when a wireless client attempts to connect to the network.

MAC-based authentication can be set up on any type of WM-AD, in addition to the Captive Portal or AAA authentication. To set up a RADIUS server for MAC-based authentication, you must set up a user account with UserID=MAC and Password=MAC (or a password defined by the administrator) for each user. Specifying a MAC address format and policy depends on which RADIUS server is being used.

If MAC-based authentication is to be used in conjunction with the 802.1X or Captive Portal authentication, an additional account with a real UserID and Password must also be set up on the RADIUS server.

MAC-based authentication responses may indicate to the Summit WM Controller what WM-AD a user should be assigned to. Authentication (if enabled) can apply on every roam.

To define MAC-based authentication for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to set up MAC-based authentication for. The **Topology** tab is displayed.

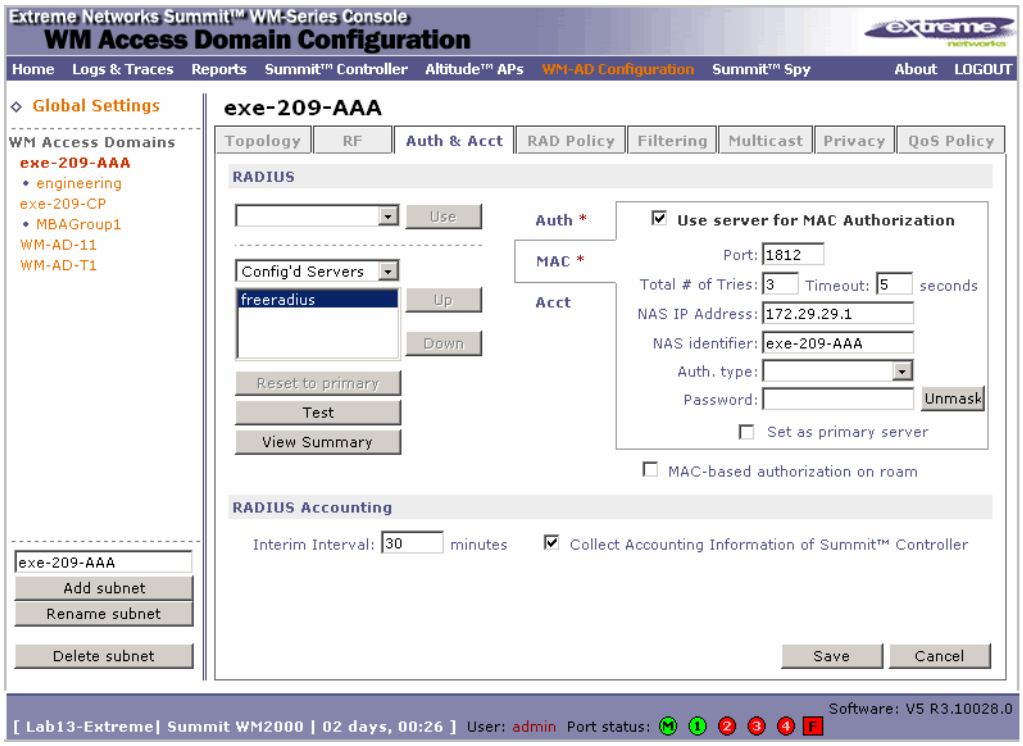
3 Click the **Auth & Acct** tab. On the **Auth & Acct** tab, there are three options:

- **Auth** - Use to define authentication servers.
- **MAC** - Use to define servers for MAC-based authentication.
- **Acct** - Use to define accounting servers.

4 Click **MAC**. The MAC fields are displayed.

5 From the **RADIUS** drop-down list, click the server you want to use for MAC authentication, and then click **Use**. The server's default information is displayed and a red asterisk is displayed next to **MAC**, indicating that a server has been assigned.

The RADIUS servers are defined on the **Global Settings** page. For more information, see "WM-AD global settings" on page 149.



6 If applicable, to use a server that has already been used for another type of authentication or accounting, click the server you want to use for MAC authentication, and then select **User server for MAC Authentication**.

7 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

8 In the **# of Retries** box, type the number of times the Summit WM Controller will attempt to access the RADIUS server.

9 In the **Timeout** box, type the maximum time, in seconds, that a Summit WM Controller will wait for a response from the RADIUS server before attempting again.

10 In the **NAS IP Address** box, type the Network Access Server (NAS) IP address.

11 In the **NAS Identifier** box, type the Network Access Server (NAS) identifier. The NAS identifier is a RADIUS attribute that identifies the server responsible for passing information to designated RADIUS servers and then acting on the response returned. This is an optional step.

12 In the **Auth. Type** field, click the authentication protocol to be used by the RADIUS server to authenticate the wireless device users for a Captive Portal WM-AD.

13 In the **Password** box, type the password you want to use for MAC-based authentication requests. The password is forwarded by the Summit WM Controller to the authentication server. If the **Password** box is left empty, the MAC address will act as the default password.

Toggle between **Mask**/**Unmask** to view and hide the defined password.

14 If applicable, select **Set as primary server**.

15 To enable MAC-based authentication on roam, select the **MAC-based authentication on roam** checkbox.

NOTE

Only select this checkbox if you are using MAC based authentication and if you want your clients to be authorized every time they roam to another AP. If this feature is not enabled, and MAC-based authentication is in use, the client is authenticated only at the start of a session.

16 To save your changes, click **Save**.

Defining accounting methods for a WM-AD

The next step in configuring a WM-AD is to define the methods of accounting. Accounting tracks the activity of a wireless device users. There are two types of accounting available:

- **Summit WM Controller accounting** - Enables the Summit WM Controller to generate Call Data Records (CDRs), containing usage information about each wireless session. CDR generation is enabled on a per WM-AD basis. For more information on CDRs, refer to "Call Detail Records (CDRs)" on page 2883.
- **RADIUS accounting** - Enables the Summit WM Controller to generate an accounting request packet with an accounting start record after successful login by the wireless device user, and an accounting stop record based on session termination. The Summit WM Controller sends the accounting requests to a remote RADIUS server.

Summit WM Controller accounting creates Call Data Records (CDRs). If RADIUS accounting is enabled, a RADIUS accounting server needs to be specified.

To define accounting methods for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define accounting methods for. The **Topology** tab is displayed.

3 Click the **Auth & Acct** tab.

4 To enable Summit WM Controller accounting, select **Collect Accounting Information of Summit Controller**.

5 From the **RADIUS** drop-down list, click the server you want to use for RADIUS accounting, and then click **Use**. The server's default information is displayed and a red asterisk is displayed next to **Acct**, indicating that a server has been assigned.

The RADIUS servers are defined on the **Global Settings** page. For more information, see "WM-AD global settings" on page 149.

6 Select **Use server for RADIUS Accounting**.

7 In the **Port** box, type the port used to access the RADIUS server. The default is 1812.

8 In the **# of Retries** box, type the number of times the Summit WM Controller will attempt to access the RADIUS server.

9 In the **Timeout** box, type the maximum time that a Summit WM Controller will wait for a response from the RADIUS server before attempting again.

10 In the **Interim Interval** box, type the time interval when accounting records are sent. Interim accounting records are sent if the interim time interval is reached before the session ends. The default is 60 minutes.

11 To save your changes, click **Save**.

Defining RADIUS filter policy for WM-ADs and WM-AD groups

The next step in configuring a WM-AD is to define the filter ID values for a WM-AD. These filter ID values must match those set up on the RADIUS servers.

NOTE

This configuration step is optional. If filter ID values are not defined, the system uses the default filter as the applicable filter group for authenticated users within a WM-AD. However, if more user-specific filter definitions are required, for example filters based on a user's department, then the filter ID configuration is used to overwrite the default assignment.

In addition to the filter ID values, you can also set up a group ID for a WM-AD with AAA authentication. You can set up a group within a WM-AD that relies on the RADIUS attribute Login-LAT-Group (RFC2865). For each group, you can define filtering rules to control access to the network.

If you define a group within an AAA WM-AD, the group (or child) definition acquires the same authentication and privacy parameters as the parent WM-AD. However, you need to define a different topology and filtering rules for this group.

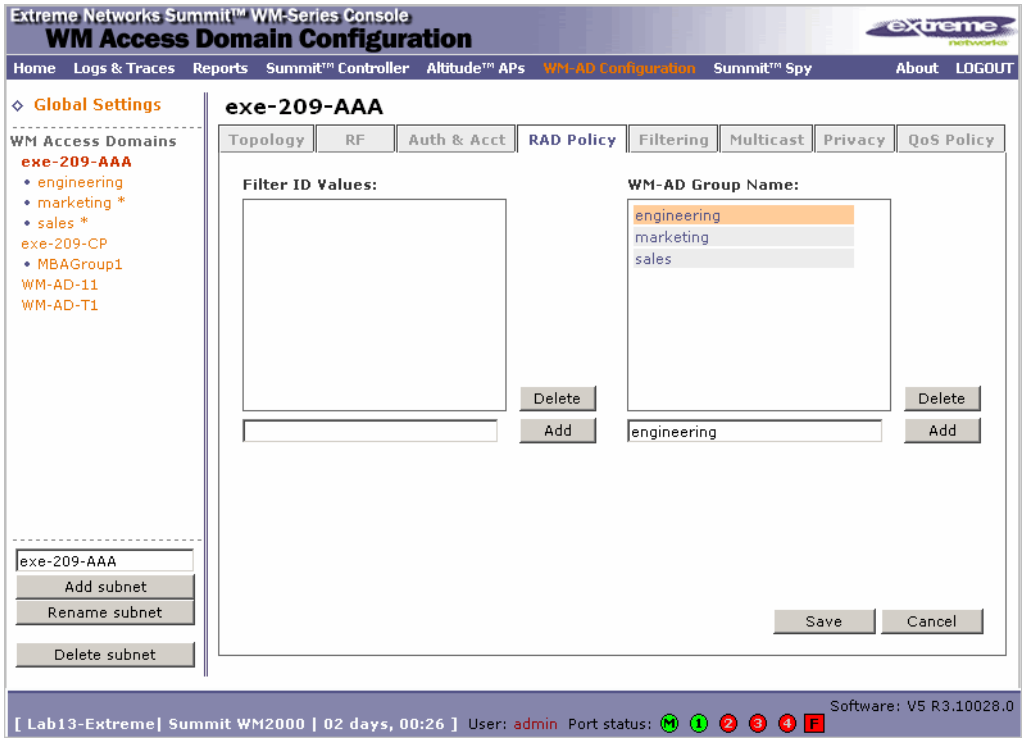
All the filters are exposed. For the Assignment by SSID with no authentication, the filter that is applied to the client session is the default filter.

To define the filter ID values on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.

3 Click the **RAD Policy** tab.



4 In the **Filter ID Values** box, type the name of a group that you want to define specific filtering rules for to control network access.

5 Click the corresponding **Add** button. The filter ID value is displayed in the list. These filter ID values will appear in the **Filter ID** list on the **Filtering** tab. These filter ID values must match those set up for the filter ID attribute in the RADIUS server.

6 If applicable, repeat steps 4 and 5 to add additional filtering ID values.

7 In the **WM-AD Group Name** box, type the name of a WM-AD group you want to create and define within the selected parent WM-AD.

8 Click the corresponding **Add** button. The Group Name will appear as a child of the parent WM-AD in the left pane **WM Access Domains** list.

9 To your changes, click **Save**.

Configuring filtering rules for a WM-AD

The next step in configuring a WM-AD is to configure the filtering rules for a WM-AD.

In an AAA WM-AD, a non-authenticated filter is unnecessary because users have already been authenticated. When authentication is returned, the filter ID group filters are applied. For AAA, a WM-AD can have a sub-group with Login-LAT-group ID that has its own filtering rules. If no filter ID matches are found, then the default filter is applied. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

Filtering rules for an exception filter

The exception filter provides a set of rules aimed at restricting the type of traffic that is delivered to the controller. By default, your system is shipped with a set of restrictive filtering rules that help control access through the interfaces to only absolutely necessary services.

By configuring to allow management on an interface, an additional set of rules is added to the shipped filter rules that provide access to the system's management configuration framework (SSH, HTTPS, SNMPAgent). Most of this functionality is handled directly behind the scenes by the system, rolling and un-rolling canned filters as the system's topology and defined access privileges for an interface change.

NOTE

*An interface for which **Allow Management** is enabled, can be reached by any other interface. By default, **Allow Management** is disabled and shipped interface filters will only permit the interface to be visible directly from it's own subnet.*

The visible exception filters definitions, both in physical ports and WM-AD definitions, allow administrators to define a set of rules to be prepended to the system's dynamically updated exception filter protection rules. Rule evaluation is performed top to bottom, until an exact match is determined. Therefor, these user-defined rules are evaluated before the system's own generated rules. As such, these user-defined rules may inadvertently create security lapses in the system's protection mechanism or create a scenario that filters out packets that are required by the system.

NOTE

Use exception filters only if absolutely necessary. It is recommended to avoid defining general allow all or deny all rule definitions since those definitions can easily be too liberal or too restrictive to all types of traffic.

The exception rules are evaluated in the context of referring to the specific controller's interface. The destination address for the filter rule definition is typically defined as the interface's own IP address. The port number for the filter definition corresponds to the target (destination) port number for the applicable service running on the controller's management plane.

The exception filter on an WM-AD applies only to the destination portion of the packet. Traffic to a specified IP address and IP port is either allowed or denied. Adding exception filtering rules allows network administrators to either tighten or relax the built-in filtering that automatically drops packets not specifically allowed by filtering rule definitions. The exception filtering rules can deny access in the event of a DoS attack, or can allow certain types of management traffic that would otherwise be denied. Typically, **Allow Management** is enabled

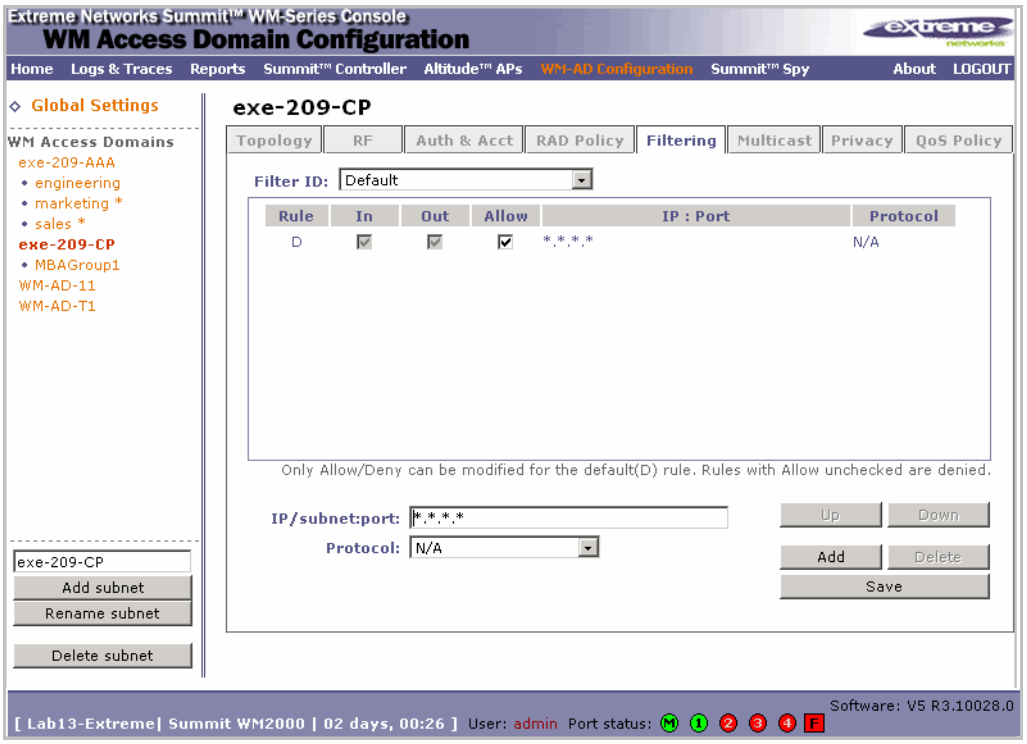
To define filtering rules for an exception filter:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.

3 Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, click **Exception**.



5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.

6 Define a rule to allow access to the default gateway for this WM-AD:

- Select **IP/Port.**
- Type the default gateway IP address (WM-AD IP address) that you defined on the **Topology** tab for this WM-AD.

7 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

8 Click the new filter, then select the **Allow** checkbox applicable to the rule you defined.

9 To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

10 To save your changes, click **Save**.

NOTE

For external Captive Portal, you need to add an external server to a non-authentication filter.

Defining non-authenticated filters

Defining non-authenticated filters allows administrators to identify destinations to which a user is allowed to access without incurring an authentication redirection. Typically, the recommended default

rule is to deny all. Administrators should define a rule set that will permit users to access essential services:

- DNS (IP of DNS server)
- Default Gateway (WM-AD Interface IP)

Any HTTP streams requested by the client for denied targets will be redirected to the specified location.

The non-authenticated filter should allow access to the Captive Portal page IP address, as well as to any URLs for the header and footer of the Captive Portal page. This filter should also allow network access to the IP address of the DNS server and to the network address - the gateway of the WM-AD. The WM-AD gateway is used as the IP for an internal Captive Portal page. An external Captive Portal will provide a specific IP definition of a server outside the Summit WM Controller.

Redirection and Captive Portal credentials apply to HTTP traffic only. A wireless device user attempting to reach Websites other than those specifically allowed in the non-authenticated filter will be redirected to the allowed destinations. Most HTTP traffic outside of those defined in the non-authenticated filter will be redirected.

NOTE

Although non-authenticated filters definitions are used to assist in the redirection of HTTP traffic for restricted or denied destinations, the non-authenticated filter is not restricted to HTTP operations. The filter definition is general. Any traffic other than HTTP that the filter does not explicitly allow will be discarded by the controller.

The non-authenticated filter is applied by the Summit WM Controller to sessions until they successfully complete authentication. The authentication procedure results in an adjustment to the user's applicable filters for access policy. The authentication procedure may result in the specification of a specific filter ID or the application of the default filter for the WM-AD.

Typically, default filter ID access is less restrictive than a non-authenticated profile. It is the administrator's responsibility to define the correct set of access privileges.

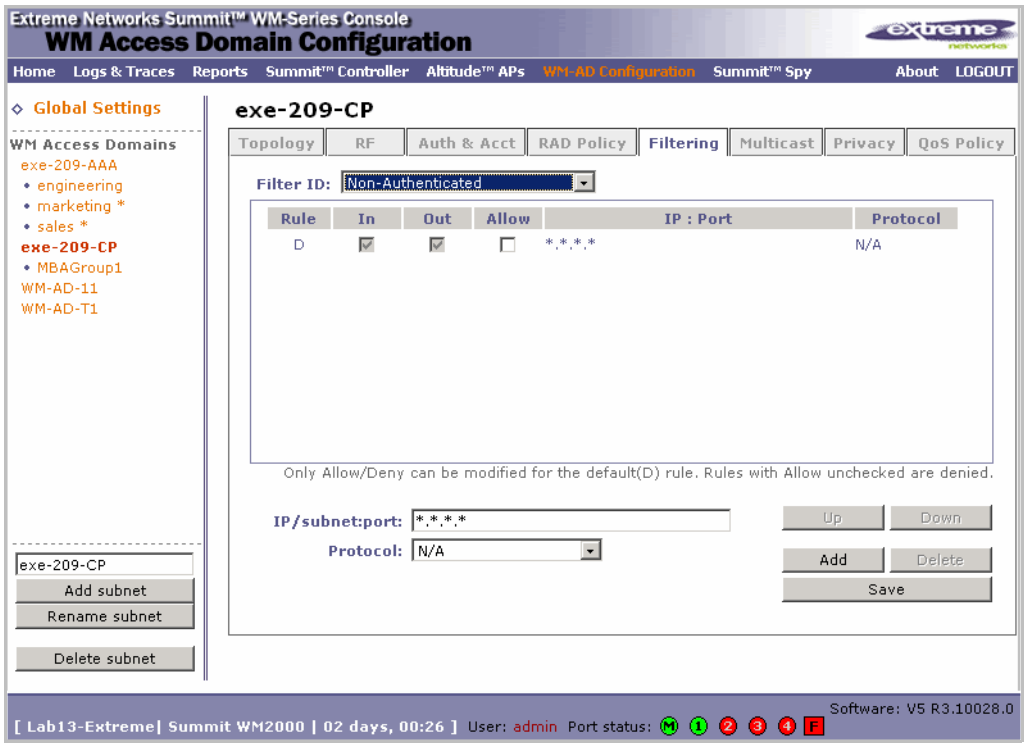
To define filtering rules for a non-authenticated filter:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define filter ID values for. The **Topology** tab is displayed.

3 Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, click **Non-Authenticated**.



The **Filtering** tab automatically provides a Deny All rule already in place. Use this rule as the final rule in the non-authenticated filter for Captive Portal.

5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.

6 For Captive Portal assignment, define a rule to allow access to the default gateway for this WM-AD:

- Select **IP/Port.**
- Type the default gateway IP address that you defined in the **Topology** tab for this WM-AD.

7 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

8 Click the new filter, then do the following:

- If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
- If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.
- Select the **Allow** checkbox applicable to the rule you defined.

9 To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

10 To save your changes, click **Save**.

NOTE

Administrators must ensure that the non-authenticated filter allows access to the corresponding authentication server:
*- **Internal Captive Portal** - IP address of the WM-AD interface*
*- **External Captive Portal** - IP address of external Captive Portal server*

Non-authenticated filter examples

A basic non-authenticated filter for internal Captive Portal should have three rules, in the following order:

Table 15: Non-authenticated filter example A

In	Out	Allow	IP/Port	Description
x	x	x	IP address of default gateway (WM-AD Interface IP)	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		*.*.*.*	Deny everything else.

NOTE

For external Captive Portal, an additional rule to Allow (in/out) access to the external Captive Portal authentication/ Web server is required.

If you place URLs in the header and footer of the Captive Portal page, you must explicitly allow access to any URLs mentioned in the authentication's server page, such as:

- **Internal Captive Portal** - URLs referenced in a header or footer
- **External Captive Portal** - URLs mentioned in the page definition

Here is another example of a non-authenticated filter that adds two more filtering rules. The two additional rules do the following:

- Deny access to a specific IP address.
- Allows only HTTP traffic.

Table 16: Non-authenticated filter example B

In	Out	Allow	IP/Port	Description
x	x	x	IP address of the default gateway	Allow all incoming wireless devices access to the default gateway of the WM-AD.
x	x	x	IP address of the DNS Server	Allow all incoming wireless devices access to the DNS server of the WM-AD.
x	x		[a specific IP address, or address plus range]	Deny all traffic to a specific IP address, or to a specific IP address range (such as:0/24).
x	x	x	*.*.*.*:80	Allow all port 80 (HTTP) traffic.
x	x		*.*.*.*	Deny everything else.

Once a wireless device user has logged in on the Captive Portal page, and has been authenticated by the RADIUS server, then the following filters will apply:

- **Filter ID** - If a filter ID associated with this user was returned by the authentication server.
- **Default filter** - If no matching filter ID was returned from the authentication server.

Filtering rules for a filter ID group

When the wireless device user provides the identification credentials, identification is sent by the Summit WM Controller to the RADIUS server, or other authentication server, through a sequence of exchanges depending on the type of authentication protocol used.

When the server allows this request for authentication - the server sends an access-accept message, the RADIUS server may also send back to the Summit WM Controller a filter ID attribute value associated with the user. For an AAA WM-AD, a Login-LAT-Group identifier for the user may also be returned. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

If the filter ID attribute value (or Login-LAT-Group attribute value) from the RADIUS server matches a filter ID value that you have set up on the Summit WM Controller, the Summit WM Controller applies the filtering rules that you defined for that filter ID value to the wireless device user.

If no filter ID is returned by the authentication server, or no match is found on the Summit WM Controller, the filtering rules in the default filter will apply to the wireless device user.

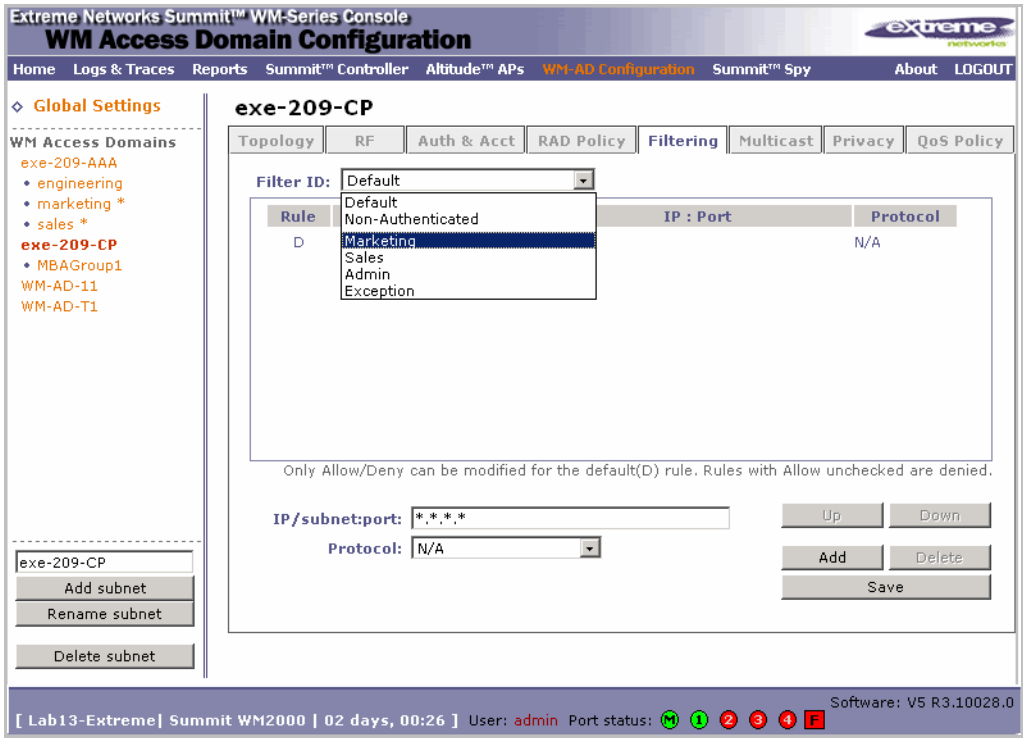
To define filtering rules for a filter ID group:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define filtering rules for a filter ID group. The **Topology** tab is displayed.

3 Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, click one of the names you defined in the **Filter ID Values** field on the **RAD Policy** tab. For example, select one of your organization's user groups, such as Sales, Engineering, Teacher, Guest, etc.



The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this WM-AD.

5 For each filtering rule you are defining, do the following:

- In the **IP/subnet:port** box, type the destination IP address. You can also specify an IP range, a port designation, or a port range on that IP address.
- In the **Protocol** drop-down list, click the applicable protocol. The default is N/A.

6 Click **Add**. The information is displayed in the **Filter Rules** section of the tab.

7 Click the new filter, then do the following:

- If applicable, select **In** to refer to traffic from the wireless device that is trying to get on the network.
- If applicable, select **Out** to refer to traffic from the network host that is trying to get to a wireless device.
- Select the **Allow** checkbox applicable to the rule you defined.

8 To edit the order of filters, click the filter, and then click the **Up** and **Down** buttons. The filtering rules are executed in the order you define here.

9 To save your changes, click **Save**.

Filtering rules by filter ID examples

Below are two examples of possible filtering rules for a filter ID. The first example disallows some specific access before allowing everything else.

Table 17: Filtering rules by filter ID example A

In	Out	Allow	IP/Port	Description
x	x		*.*.*.*:22-23	SSH and telnet sessions
x	x		[specific IP address, range]	Deny all traffic to a specific IP address or address range
x	x	x	*.*.*.*.	Allow everything else

The second example does the opposite of the first example. It allows some specific access and denies everything else.

Table 18: Filtering rules by filter ID example B

In	Out	Allow	IP/Port	Description
x	x	x	[specific IP address, range]	Allow traffic to a specific IP address or address range.
x	x		*.*.*.*.	Deny everything else.

Filtering rules for a default filter

After authentication of the wireless device user, the default filter will apply only after:

- No match is found for the Exception filter rules.
- No filter ID attribute value is returned by the authentication server for this user.
- No match is found on the Summit WM Controller for a filter ID value.

The final rule in the default filter should be a catch-all rule for any traffic that did not match a filter. A final Allow All rule in a default filter will ensure that a packet is not dropped entirely if no other match can be found. WM-AD Policy is also applicable for Captive Portal and MAC-based authorization.

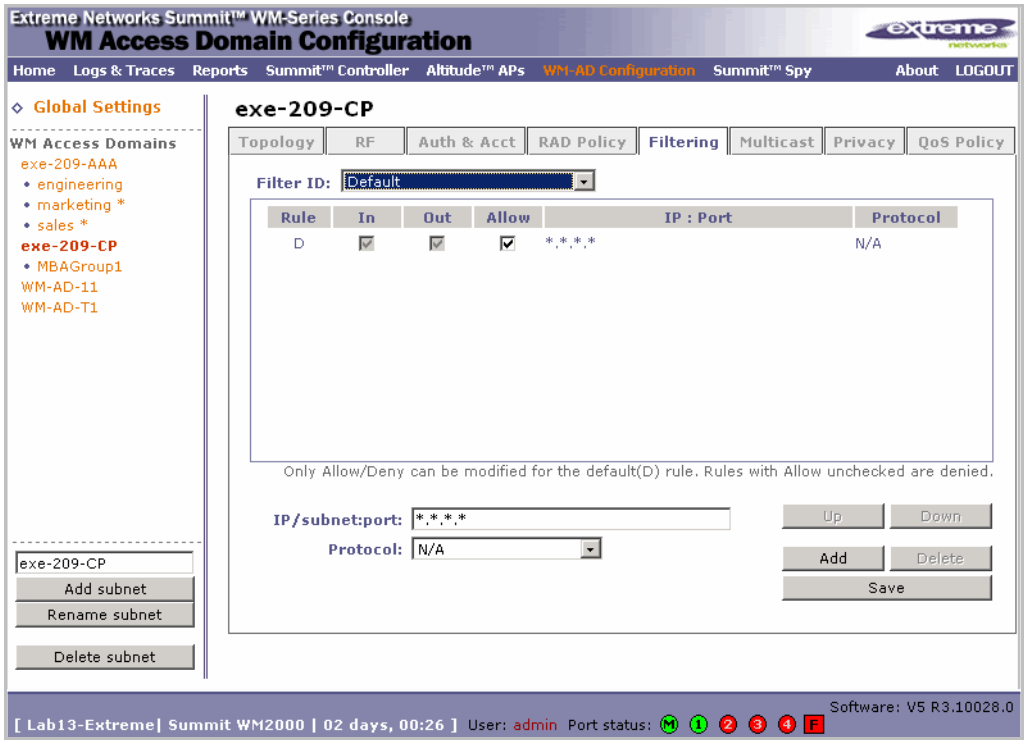
To define the filtering rules for a default filter:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to define the filtering rules for a default filter. The **Topology** tab is displayed.

3 Click the **Filtering** tab.

4 From the **Filter ID** drop-down list, click **Default**.



The **Filtering** tab automatically provides a Deny All rule already in place. This rule can be modified to Allow All, if appropriate to the network access needs for this WM-AD.

Default filter examples

The following are examples of filtering rules for a default filter:

Table 19: Default filter example A

In	Out	Allow	IP / Port	Description
x	x		Intranet IP, range	Deny all access to an IP range
x	x		Port 80 (HTTP)	Deny all access to Web browsing
x	x		Intranet IP	Deny all access to a specific IP
x	x	x	*.*.*.*.	Allow everything else

Table 20: Default filter example B

In	Out	Allow	IP / Port	Description
x			Port 80 (HTTP) on host IP	Deny all incoming wireless devices access to Web browsing the host
	x		Intranet IP 10.3.0.20, ports 10-30	Deny all traffic from the network to the wireless devices on the port range, such as TELNET (port 23) or FTP (port 21)
x		x	Intranet IP 10.3.0.20	Allow all other traffic from the wireless devices to the Intranet network

Table 20: Default filter example B (Continued)

In	Out	Allow	IP / Port	Description
	x	x	Intranet IP 10.3.0.20	Allow all other traffic from Intranet network to wireless devices
x	x	x	*.*.*.*.	Allow everything else

Filtering rules for an AAA child group WM-AD

If you defined a child group for an AAA WM-AD, it will have the same authentication parameters and filter IDs as the parent WM-AD. However, you can define different filtering rules for the filters IDs in the child configuration from those in the parent configuration.

Filtering rules between two wireless devices

Traffic from two wireless devices that are on the same WM-AD and are connected to the same Altitude AP will pass through the Summit WM Controller and therefore be subject to filtering policy. You can set up filtering rules that allow each wireless device access to the default gateway, but also prevent each device from communicating with each other.

Add the following two rules to a filter ID filter, before allowing everything else:

Table 21: Rules between two wireless devices

In	Out	Allow	IP / Port	Description
x	x	x	[Intranet IP]	Allow access to the Gateway IP address of the WM-AD only
x	x		[Intranet IP, range]	Deny all access to the WM-AD subnet range (such as 0/24)
x	x	x	*.*.*.*.	Allow everything else

Enabling multicast for a WM-AD

A mechanism that supports multicast traffic can be enabled as part of a WM-AD definition. This mechanism is provided to support the demands of VoIP and IPTV network traffic, while still providing the network access control.

NOTE

*To use the mobility feature with this WM-AD, you must select the **Enable Multicast Support** checkbox for the data port.*

Define a list of multicast groups whose traffic is allowed to be forwarded to and from the WM-AD. The default behavior is to drop the packets. For each group defined, you can enable Multicast Replication by group.

NOTE

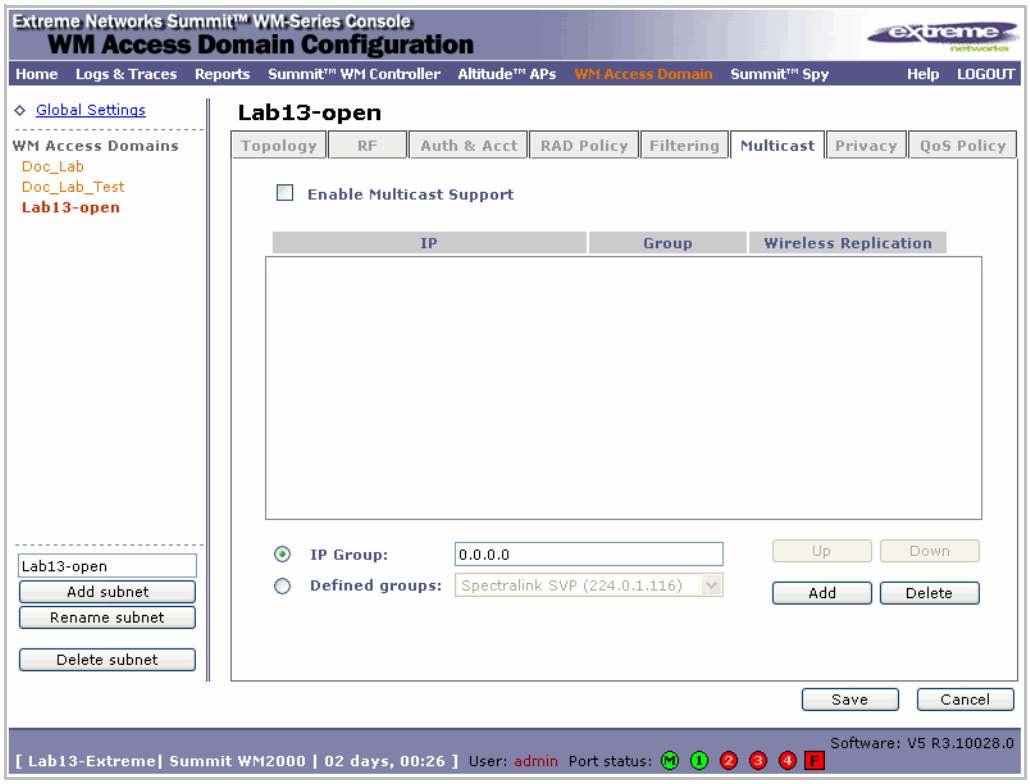
*Before enabling multicast filters and depending on the topology of the WM-AD, you may need to define which physical interface to use for multicast relay. Define the multicast port on the **IP Addresses** page. For more information, see "Setting up the data ports" on page 36.*

To enable multicast for a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to enable Multicast for. The **Topology** tab is displayed.

3 Click the **Multicast** tab.



4 To enable the multicast function, select **Enable Multicast Support**.

5 Define the multicast groups by selecting one of the radio buttons:

- **IP Group** - Type the IP address range.
- **Defined groups** - Click from the drop-down list.

6 Click **Add**. The group is added to the list above.

7 To enable the wireless multicast replication for this group, select the corresponding **Wireless Replication** checkbox.

8 To modify the priority of the multicast groups, click the group row, and then click the **Up** or **Down** buttons.

A Deny All rule is automatically added as the last rule, IP = *.*.*.* and the **Wireless Replication** checkbox is not selected. This rule ensures that all other traffic is dropped.

9 To save your changes, click **Save**.

NOTE

The multicast packet size should not exceed 1450 bytes.

Configuring privacy for a WM-AD

Privacy is a mechanism that protects data over wireless and wired networks, usually by encryption techniques. The following section describes how the Privacy mechanism is handled for a Captive Portal WM-AD and an AAA WM-AD.

NOTE

Regardless of the Altitude AP model or WM-AD type, a maximum of 112 simultaneous clients, per radio, are supported by all of the data protection encryption techniques listed below.

Privacy for a WM-AD for Captive Portal

For the Captive Portal WM-AD, there are three options for the privacy mechanism:

- **None**
- **Static Wired Equivalent Privacy (WEP)** - Keys for a selected WM-AD, so that it matches the WEP mechanism used on the rest of the network. Each radio can support up to eight SSIDs (16 SSIDs per AP). Each AP can participate in up to 50 WM-ADs. For each WM-AD, only one WEP key can be specified. It is treated as the first key in a list of WEP keys.
- **Wi-Fi Protected Access (WPA) Pre-Shared key (PSK)** - Privacy in PSK mode, using a Pre-Shared Key (PSK), or shared secret for authentication. WPA-PSK is a security solution that adds authentication to enhanced WEP encryption and key management. WPA-PSK mode does not require an authentication server. It is suitable for home or small office.

Altitude 802.11n APs and WPA authentication

If a WM-AD is configured to use WPA authentication, any Altitude 802.11n AP within that WM-AD will do the following:

- WPA v.1 - If WPA v.1 is enabled, the Altitude 802.11n AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 - If WPA v.2 is enabled, the Altitude 802.11n AP will do the following:
  - If WPA v.1 is enabled, the Altitude 802.11n AP will advertise TKIP as an available encryption protocol.

NOTE

If WPA v.2 is enabled, the Wireless 802.11n AP does not support the Auto option.

- If WPA v.1 is disabled, the Altitude 802.11n AP will advertise the encryption cipher AES (Advanced Encryption Standard).

NOTE

The security encryption for some network cards must not to be set to WEP or TKIP to achieve a data rate beyond 54 Mbps.

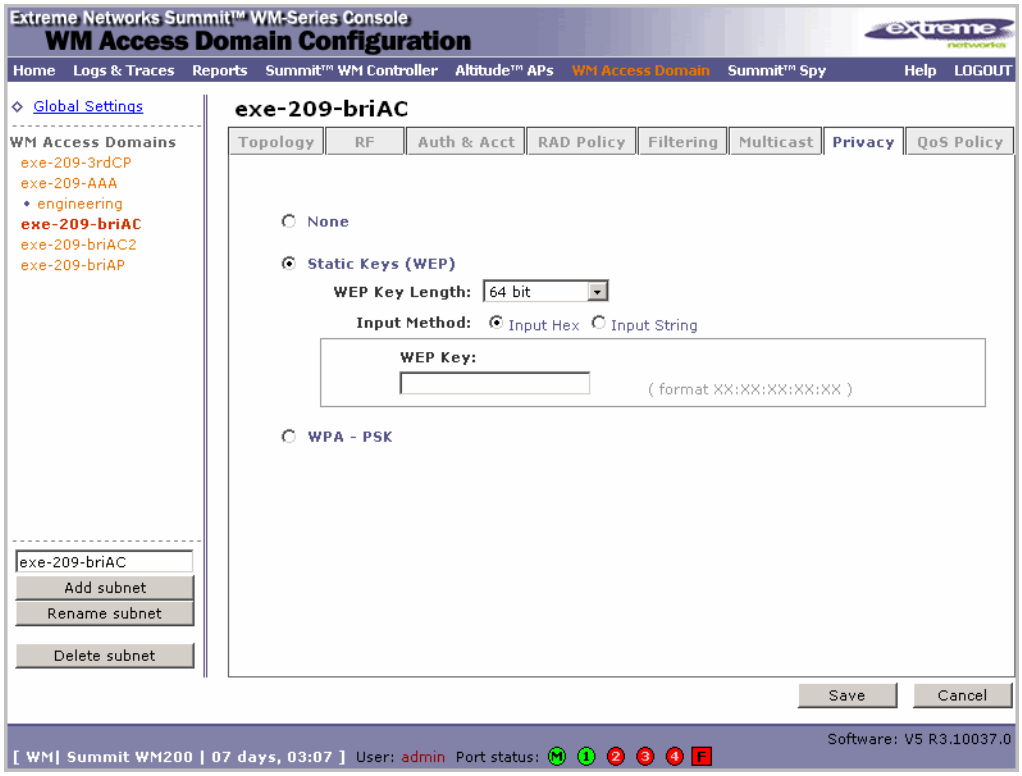
To configure privacy by static WEP for a Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure privacy by static WEP for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

4 Select **Static Keys (WEP)**.



5 From the **WEP Key Length** drop-down list, click the WEP encryption key length:

- 64-bit
- 128-bit
- 152-bit

6 Select one of the following input methods:

- **Input Hex** - If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.

- **Input String** - If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.

7 To save your changes, click **Save**.

To configure privacy by WPA-PSK for a Captive Portal WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

4 Select **WPA-PSK**.

5 To enable WPA v1 encryption, select **WPA v.1**.

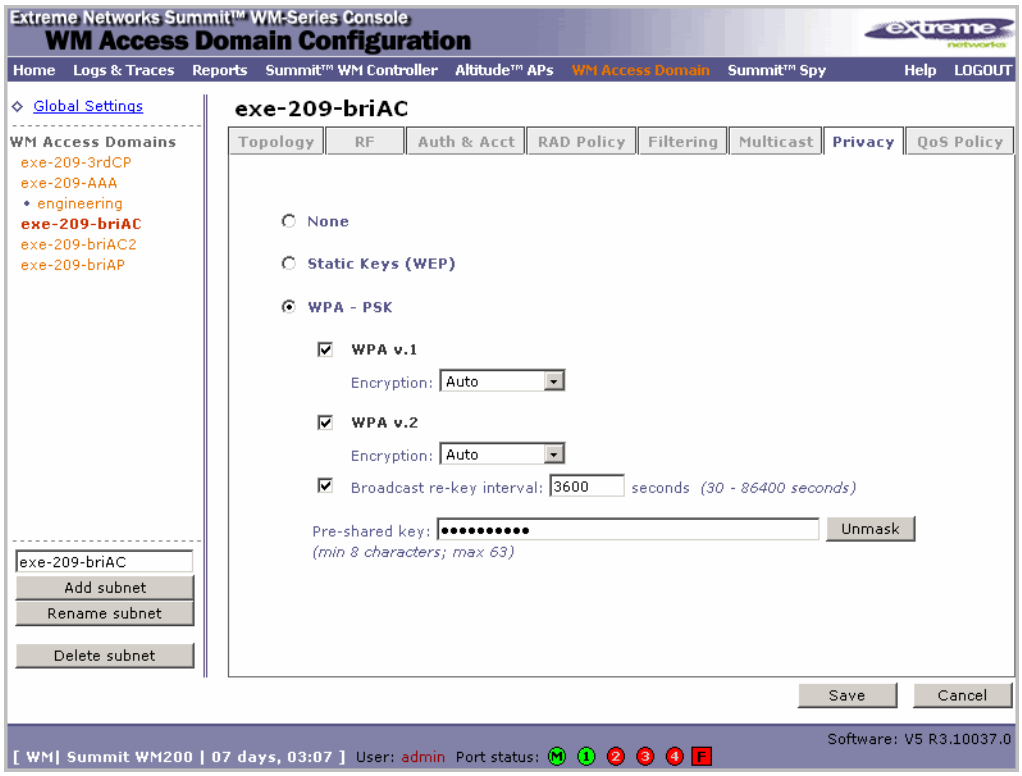
6 If WPA v.1 is enabled, click one of the following encryption types from the **Encryption** drop-down list:

- **Auto** - The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
- **TKIP only** - The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.

7 To enable WPA v2-type encryption, select **WPA v.2**.

The other options for this drop-down list are:

- **Auto** - If you click Auto, the Altitude AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
- **AES only** - If you click AES, the Altitude AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.



8 To enable re-keying after a time interval, select **Broadcast re-key interval**.

If this checkbox is not selected, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.

9 In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.

10 In the **Pre-Shared Key** box, type the shared secret key to be used between the wireless device and Altitude AP. The shared secret key is used to generate the 256-bit key.

11 To proofread your entry before saving the configuration, click **Unmask** to display the Pre-Shared Key. To mask the key, click **Mask**.

12 To save your changes, click **Save**.

Privacy for a WM-AD for AAA

For a WM-AD with authentication by 802.1X (AAA), there are four Privacy options:

- Static keys (WEP)
- Dynamic keys
- Wi-Fi Protected Access (WPA) version 1, with encryption by Temporal Key Integrity Protocol (TKIP)
- Wi-Fi Protected Access (WPA) version 2, with encryption by Advanced Encryption Standard with Counter-Mode/CBC-MAC Protocol (AES-CCMP)

NOTE

In order to use WPA with 802.1X authentication, network assignment must be AAA.

Altitude 802.11n APs and WPA authentication

If a WM-AD is configured to use WPA authentication, any Altitude 802.11n AP within that WM-AD will do the following:

- WPA v.1 - If WPA v.1 is enabled, the Altitude 802.11n AP will advertise only TKIP as an available encryption protocol.
- WPA v.2 - If WPA v.2 is enabled, the Altitude 802.11n AP will do the following:
  - If WPA v.1 is enabled, the Altitude 802.11n AP will advertise TKIP as an available encryption protocol.

NOTE

If WPA v.2 is enabled, the Wireless 802.11n AP does not support the Auto option.

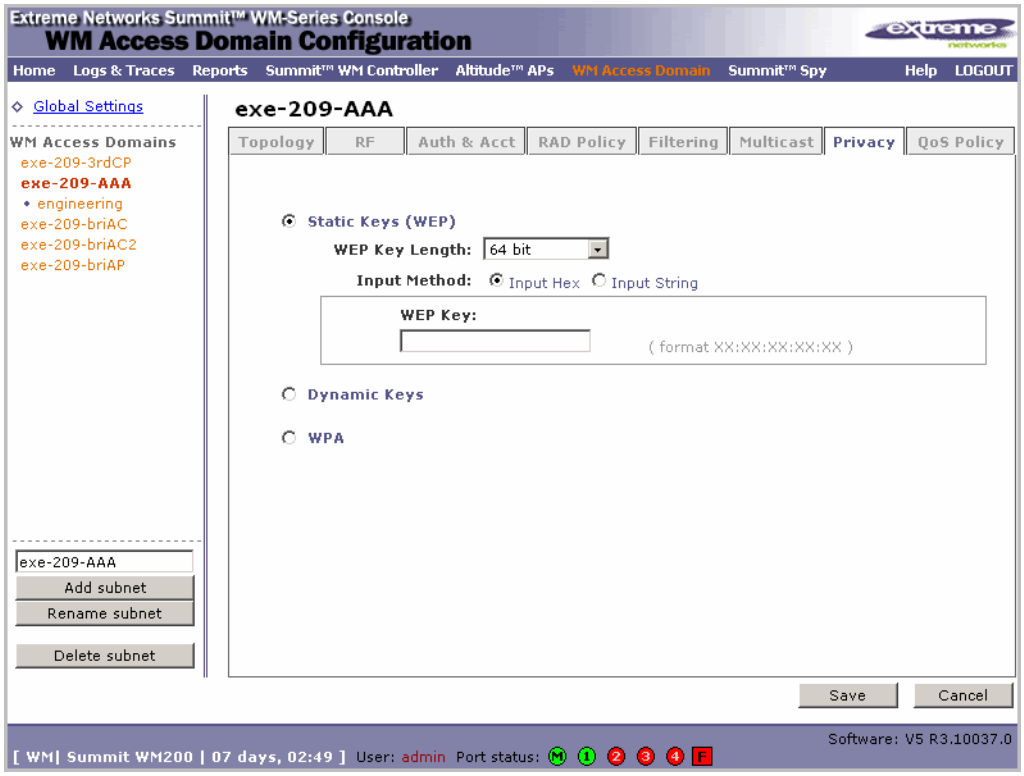
  - If WPA v.1 is disabled, the Altitude 802.11n AP will advertise the encryption cipher AES (Advanced Encryption Standard).

To set up static WEP privacy for an AAA WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the AAA WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.

3 Click the **Privacy** tab.



4 Select **Static Keys (WEP)**.

5 From the **WEP Key Length** drop-down list, click the WEP encryption key length:
   - 64-bit
   - 128-bit
   - 152-bit

6 Select one of the following input methods:
   - **Input Hex** - If you select **Input Hex**, type the WEP key input in the **WEP Key** box. The key is generated automatically, based on the input.
   - **Input String** - If you select **Input String**, type the secret WEP key string used for encrypting and decrypting in the **WEP Key String** box. The WEP Key box is automatically filled by the corresponding Hex code.

7 To save your changes, click **Save**.

Dynamic WEP privacy for an AAA WM-AD

The dynamic key WEP mechanism changes the key for each user and each session.

To set up dynamic WEP privacy for a selected AAA WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the AAA WM-AD you want to set up dynamic WEP privacy for. The **Topology** tab is displayed.

3 Click the **Privacy** tab.

4 Select **Dynamic Keys**.

5 To save your changes, click **Save**.

Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy for an AAA WM-AD

The WM-AD Privacy feature supports Wi-Fi Protected Access (WPA v1 and WPA v2), a security solution that adds authentication to enhanced WEP encryption and key management.

The authentication portion of WPA for AAA is in Enterprise Mode:

- Specifies 802.1X with Extensible Authentication Protocol (EAP)
- Requires a RADIUS or other authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes management of user credentials

The encryption portion of WPA v1 is Temporal Key Integrity Protocol (TKIP). TKIP includes:

- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet (unicast key) or after the specified re-key time interval (broadcast key) expires
- An extended WEP key length of 256-bits
- An enhanced Initialization Vector (IV) of 48 bits, instead of 24 bits, making it more difficult to compromise

- A Message Integrity Check or Code (MIC), an additional 8-byte code that is inserted before the standard WEP 4-byte Integrity Check Value (ICV). These integrity codes are used to calculate and compare, between sender and receiver, the value of all bits in a message, which ensures that the message has not been tampered with.

The encryption portion of WPA v2 is Advanced Encryption Standard (AES). AES includes:

- A 128 bit key length, for the WPA2/802.11i implementation of AES
- Four stages that make up one round. Each round is iterated 10 times.
- A per-packet key mixing function that shares a starting key between devices, and then changes their encryption key for every packet or after the specified re-key time interval expires.
- The Counter-Mode/CBC-MAC Protocol (CCMP), a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include:
  - Counter mode (CTR) that achieves data encryption
  - Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity

The following is an overview of the WPA authentication and encryption process:

- **Step one** - The wireless device client associates with Altitude AP.
- **Step two** - Altitude AP blocks the client's network access while the authentication process is carried out (the Summit WM Controller sends the authentication request to the RADIUS authentication server).
- **Step three** - The wireless client provides credentials that are forwarded by the Summit WM Controller to the authentication server.
- **Step four** - If the wireless device client is not authenticated, the wireless client stays blocked from network access.
- **Step five** - If the wireless device client is authenticated, the Summit WM Controller distributes encryption keys to the Altitude AP and the wireless client.
- **Step six** - The wireless device client gains network access via the Altitude AP, sending and receiving encrypted data. The traffic is controlled with permissions and policy applied by the Summit WM Controller.

Key Management Options

Wi-Fi Protected Access (WPA v1 and WPA v2) Privacy offers you the following key management options:

- None
- Opportunistic Keying
- Pre-authentication
- Opportunistic Keying & Pre-auth

The following sections explain the key management options.

None

The wireless client device performs a complete 802.1X authentication each time it associates or tries to connect to an Altitude AP.

Opportunistic Keying

Opportunistic Keying or opportunistic key caching (OKC) enables the client devices to roam fast and securely from one Altitude AP to another in 802.1X authentication setup.

The client devices that run applications such as video streaming and VoIP require rapid reassociation during roaming. OKC helps such client devices by enabling them to rapidly reassociate with the Altitude APs. This avoids delays and gaps in transmission and thus helps in secure fast roaming (SFR).

NOTE

The client devices should support OKC to use the OKC feature in the Summit WLAN.

Pre-authentication

Pre-authentication enables a client device to authenticate simultaneously with multiple Altitude APs in 802.1X authentication setup. When the client device roams from one Altitude AP to another, it does not have to perform the complete 802.1X authentication to reassociate with the new Altitude AP as it is already pre-authenticated with it. This reduces the reassociation time and thus helps in seamless roaming.

NOTE

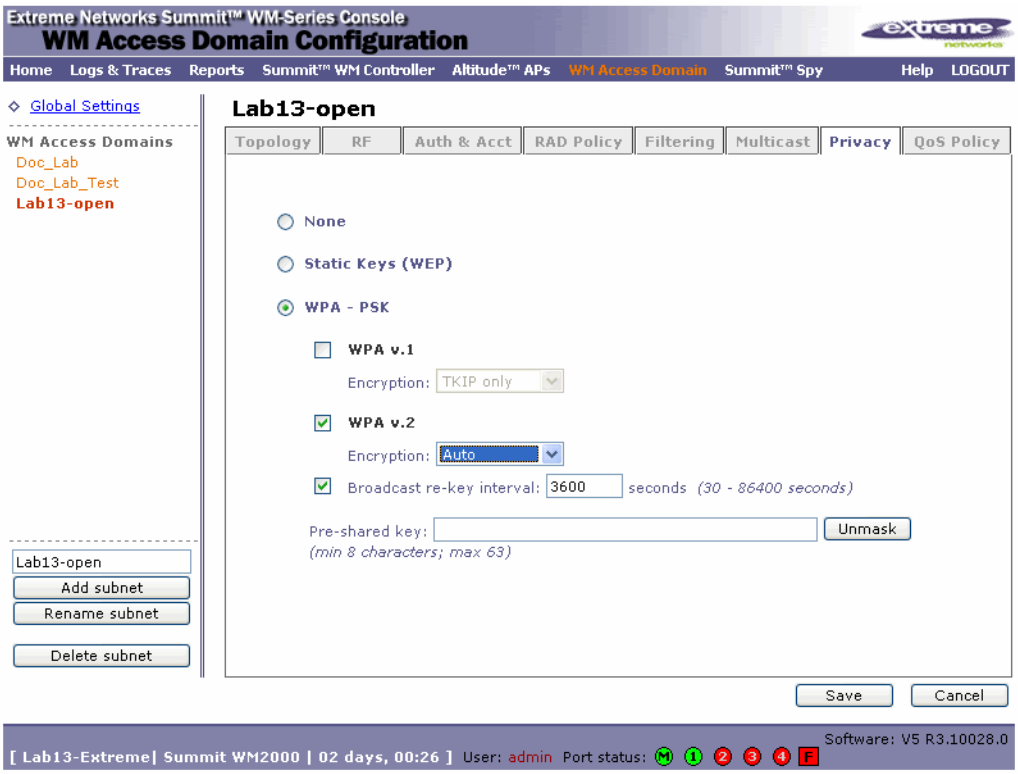
The client devices should support pre-authentication to use the pre-authentication feature in Summit WLAN.

Opportunistic Keying & Pre-auth

Opportunistic Keying and Pre-auth options is meant for the device clients that support both the authentication processes. For example, the Microsoft-operated device clients support opportunistic keying by default, but they can be configured to support pre-authentication too.

To set up Wi-Fi Protected Access privacy (WPA) for an AAA WM-AD:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.
2. In the left pane **WM Access Domains** list, click the AAA WM-AD you want to configure privacy by WPA-PSK for a Captive Portal. The **Topology** tab is displayed.
3. Click the **Privacy** tab.
4. Select **WPA**.



5 To enable WPA v1 encryption, select **WPA v.1**.

- From the **Encryption** drop-down list, select one of the following encryption types:
  - **Auto** - The AP will advertise both TKIP and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) for WPAv1. CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
  - **TKIP only** - The AP will advertise TKIP as an available encryption protocol for WPAv1. It will not advertise CCMP.

6 To enable WPA v2 encryption, select **WPA v.2**.

- From the **Encryption** drop-down list, click one of the following encryption types:
  - **Auto** - The AP advertises both TKIP and CCMP (counter mode with cipher block chaining message authentication code protocol). CCMP is an IEEE 802.11i encryption protocol that uses the encryption cipher AES (Advanced Encryption Standard). Auto is the default.
  - **AES only** - The AP advertises CCMP as an available encryption protocol. It will not advertise TKIP.
- From the **Key Management options**, click one of the following key management options:
  - **None** - The mobile units (client devices) performs a complete 802.1X authentication each time it associates or connects to an Altitude AP.
  - **Opportunistic Keying** - Enables secure fast roaming (SFR) of mobile units. For more information, see "Opportunistic Keying" on page 200.
  - **Pre-authentication** - Enables seamless roaming. For more information, see "Pre-authentication" on page 200.
  - **Opportunistic Keying & Pre-auth** - For more information, see "Opportunistic Keying & Pre-auth" on page 200.

7 To enable re-keying after a time interval, select **Broadcast re-key interval**.

If this checkbox is not selected, the Broadcast encryption key is never changed and the Altitude AP will always use the same broadcast key for Broadcast/Multicast transmissions. This will reduce the level of security for wireless communications.

8 In the **Broadcast re-key interval** box, type the time interval after which the broadcast encryption key is changed automatically. The default is 3600.

9 To save your changes, click **Save**.

Defining a WM-AD with no authentication

You can set up a WM-AD that will bypass all authentication mechanisms and run Controller, Access Points and Convergence Software with no authentication of a wireless device user.

A WM-AD with no authentication can still control network access using filtering rules. For more information on how to set up filtering rules that allow access only to specified IP addresses and ports, see "Defining non-authenticated filters" on page 183.

To define a WM-AD with no authentication:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box.

3 Click **Add subnet**. The name is displayed in the **WM Access Domains** list. The Topology tab is displayed.

4 From the **Assignment by** drop-down list, click **SSID**.

5 Configure the topology for this WM-AD, and then click **Save**. For more information, see "Configuring topology for a WM-AD for Captive Portal" on page 157.

You must save your changes before moving to the next tab.

6 Click the **Auth & Acct** tab.

7 Click **Configure Captive Portal Settings**. The **Captive Portal Configurations** window is displayed.

8 Select **No Captive Portal Support**. You must save your changes before moving to the next tab.

9 Click the **Filtering** tab.

10 Define a default filter that will control specific network access for any wireless device users on this WM-AD. For more information, see "Configuring filtering rules for a WM-AD" on page 181.

These rules should be very restrictive and the final rule should be a Deny All rule. The non-authenticated filter for a WM-AD with no authentication will not have a Captive Portal page for login.

11 To save your changes, click **Save**.

Defining priority level and service class for WM-AD traffic

Voice over Internet Protocol (VoIP) using 802.11 wireless local area networks are enabling the integration of internet telephony technology on wireless networks. Various issues including Quality-of-Service (QoS), call control, network capacity, and network architecture are factors in VoIP over 802.11 WLANs.

Wireless voice data requires a constant transmission rate and must be delivered within a time limit. This type of data is called isochronous data. This requirement for isochronous data is in contradiction to the concepts in the 802.11 standard that allow for data packets to wait their turn, in order to avoid data collisions. Regular traffic on a wireless network is an asynchronous process in which data streams are broken up by random intervals.

To reconcile the needs of isochronous data, mechanisms are added to the network that give voice data traffic or another traffic type priority over all other traffic, and allow for continuous transmission of data.

In order to provide better network traffic flow, the Controller, Access Points and Convergence Software provides advanced Quality of Service (QoS) management. These management techniques include:

- **WMM (Wi-Fi Multimedia)** - Enabled on individual Altitude AP, the standard provides multimedia enhancements that improve the user experience for audio, video, and voice applications. WMM is part of the 802.11e standard for QoS.
- **IP ToS (Type of Service) or DSCP (Diffserv Codepoint)** - The ToS/DSCP field in the IP header of a frame is used to indicate the priority and Quality of Service for each frame. The IP TOS and/or DSCP is maintained within CTP (CAPWAP Tunneling Protocol) by copying the user IP QoS information to the CTP header - this is referred to as Adaptive QoS.

Defining the service class for the WM-AD

Service class is determined by the combination of the following operations:

- The class of treatment given to a packet. For example, queuing or per hop behavior (PHB).
- The packet marking of the output packets (user traffic and/or transport).

Table 22: Service classes

Service class name (number)	Priority level
Network Control (7)	7 (highest priority)
Premium (Voice) (6)	6
Platinum (video) (5)	5
Gold (4)	4
Silver (3)	3
Bronze (2)	2
Best Effort (1)	1
Background (0)	0 (lowest priority)

The service class is equivalent to the 802.1D UP (user priority) with the exception that its scale is linear:

Table 23: Relationship between service class and 802.1D UP

SC name	SC Value	802.1d UP	AC	Queue
Network Control	7	7	VO	VO or TVO
Premium (voice)	6	6	VO	VO or TVO
Platinum (video)	5	5	VI	VI
Gold	4	4	VI	VI
Silver	3	3	BE	BE
Bronze	2	0	BE	BE
Best Effort	1	2	BK	BK
Background	0	1	BK	BK

Configuring the priority override

Priority override allows you to define the desired priority level. Priority override can be used with any combination, as shown in Table 24. You can configure the service class (L2 override) and the DSCP values (L3 override values).

When **Priority Override** is enabled, the configured service class overrides the queue selection in the downlink direction, the 802.1P UP for the VLAN tagged Ethernet packets, and the UP for the wireless QoS packets (WMM or 802.11e) according to the mapping in Table 23. If **Priority Override** is enabled and the WM-AD is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

Working with Quality of Service (QoS)

QoS policy is configured for each WM-AD and applies to routed, bridged at AP, and bridged at controller WM-ADs.

Each WM-AD has a configurable policy for the QoS characteristics of the WM-AD. For every user associated with the WM-AD there will be a different behavior on the wireless traffic.

NOTE

Active QoS is only applied on the wireless/802.11 domain, not on the wired domain.

QoS modes

You can enable the following Qos modes for a WM-AD:

- **Legacy** - If enabled, the AP will classify and prioritize the downlink traffic for all clients according to the same rules used for the WMM and 802.11e.
- **WMM** - If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all WMM clients. WMM clients will also classify and prioritize the uplink traffic.

- **802.11e** - If enabled, the AP will accept WMM client associations, and will classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic.
- **Turbo Voice** - If any of the above QoS modes are enabled, the Turbo Voice mode is available. If enabled, all the downlink traffic that is classified to the Voice (VO) AC and belongs to that WM-AD is transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. The TVO queue is tailored in terms of contention parameters and number of retries to maximize voice quality and voice capacity.

All combinations of the three modes are valid. The following table summarizes all possible combinations:

Table 24: QoS mode combinations

Configuration	Legacy mode	x		x		x		x
	WMM mode		x	x			x	x
	802.11e mode				x	x	x	x
Traffic that is classified and prioritized	To legacy client	x		x		x		x
	From legacy client							
	To WMM client	x	x	x		x	x	x
	From WMM client		x	x			x	x
	To 802.11e client	x		x	x	x	x	x
	From 802.11e client				x	x	x	x

The APs are capable of supporting 5 queues. The queues are implemented per radio. For example, 5 queues per radio. The queues are:

Table 25: Queues

Queue Name	Purpose
AC_VO	Voice
AC_VI	Video
AC_BK	Background
AC_BE	Best Effort
AC_TVO	Turbo Voice

The Summit WM Controller supports the definition of 8 levels of user priority (UP). These priority levels are mapped at the AP to the best appropriate access class. Of the 8 levels of user priority, 6 are considered low priority levels and 2 are considered high priority levels.

WMM clients have the same 5 AC queues. WMM clients will classify the traffic and use these queues when they are associated with a WMM-enabled AP. WMM clients will behave like non-WMM clients - map all traffic to the Best Effort (BE) queue - when not associated with WMM-enabled AP.

The prioritization of the traffic on the downstream (for example, from wired to wireless) and on the upstream (for example, from wireless to wired) is dictated by the configuration of the WM-AD and the QoS tagging within the packets, as set by the wireless devices and the host devices on the wired network.

Both Layer 3 tagging (DSCP) and Layer 2 (802.1d) tagging are supported, and the mapping is conformant with the WMM specification. If both L2 and L3 priority tags are available, then both are

taken into account and the chosen AC is the highest resulting from L2 and L3. If only one of the priority tags is present, it is used to select the queue. If none is present, the default queue AC_BE is chosen.

NOTE

If the wireless packets to be transmitted must include the L2 priority (send to a WMM client from a WMM-enabled AP), the outbound L2 priority is copied from the inbound L2 priority if available, or it is inferred from the L3 priority using the above table if the L2 inbound priority is missing.

Table 26: Traffic prioritization

WM-AD type	Packet Source	Packet type	L2	L3
Tunneled	Wired	Untagged	No	Yes
Branch	Wired	VLAN tagged	Yes	Yes
Branch	Wired	Untagged	No	Yes
Branch or Tunneled	Wireless	WMM	Yes	Yes
Branch or Tunneled	Wireless	non-WMM	No	Yes

Configuring the QoS policy on a WM-AD

The following is an overview of the steps involved in configuring the QoS on a WM-AD.

Step one - Define the QoS mode to employ on the WM-AD:

- **Legacy** - Enables DL (downlink) classification for all clients
- **WMM**:
  - Enables WMM support
  - Enables DL classification for WMM clients
  - Enables UL (uplink) classification in WMM clients
- **802.11e**:
  - Enables 802.11e support
  - Enables DL classification for 802.11e clients
  - Enables UL classification in 802.11e clients

  WMM and 802.11e are similar but, they use different signaling (same as WPA and WPA2).

Step 2 - Enabling Turbo Voice:

- Ensures WM-AD is optimized for voice performance and capacity
- Can be enabled or disabled on individual WM-ADs
  - If Turbo Voice is enabled, together with QoS modes **Legacy**, **WMM**, or **802.11e**, DL voice traffic is sent via Turbo Voice queue instead of voice queue. A separate turbo voice queue allows for some

WM-ADs to use the Turbo Voice parameters for voice traffic, while other WM-ADs use the voice parameters for voice traffic.

- If WMM mode is also enabled, WMM clients use Turbo Voice-like contention parameters for UL voice traffic.
- If 802.11e mode is also enabled, 802.11e clients use Turbo Voice-like contention parameters for UL voice traffic.

NOTE

The Wireless 802.11n AP does not support the Turbo Voice option.

Step 3 - Defining the DSCP and service class classifications:

All 64 DSCP code-points are supported. The IETF defined codes are listed by name and code. Undefined codes are listed by code. The following is the default DSCP service class classification:

DSCP	SC/UP	DSCP	SC/UP	DSCP	SC/UP
CS0/DE	2/0	AF11	2/0	AF33	4/4
CS1	0/1	AF12	2/0	AF41	5/5
CS2	1/2	AF13	2/0	AF42	5/5
CS3	3/3	AF21	3/3	AF43	5/5
CS4	4/4	AF22	3/3	EF	6/6
CS5	5/5	AF23	3/3	Others	0/1
CS6	6/6	AF31	4/4		
CS7	7/7	AF32	4/4		

Step 4 - Enable Priority override:

- Click the applicable service class and implicitly desired UP
  - Updates UP in user packet
  - Updates UP for WASSP frame (if field exists) sent by AP
- Select the desired DSCP
  - Updates DSCP for WASSP frames sent by AP
  - Does not change DSCP in user packet

Step 5 - Configure the advanced wireless QoS:

- Enable the **Unscheduled Automatic Power Save Delivery** (U-APSD) feature
- Works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled

Step 6 - Configure Global Admission Control:

- Enable admission control. Admission control protects admitted traffic against new bandwidth demands. Admission control is available for Voice and Video.

- If admission control is enabled, you can configure the UL and DL policer action.
- The UL and DL policers act as enforcement of a traffic management system. Depending on the TSPEC negotiation per traffic class, Voice and Video, you can configure what actions the Altitude AP takes when admitted traffic has violated its TSPEC.
  - You can configure the UL and DL policers per WM-AD
  - TSPEC statistics can be viewed in the Admission Control Statistics by Altitude AP display. For more information, see Chapter 10, "Working with reports and displays.".

Step 7 - Apply Bandwidth Control Profile

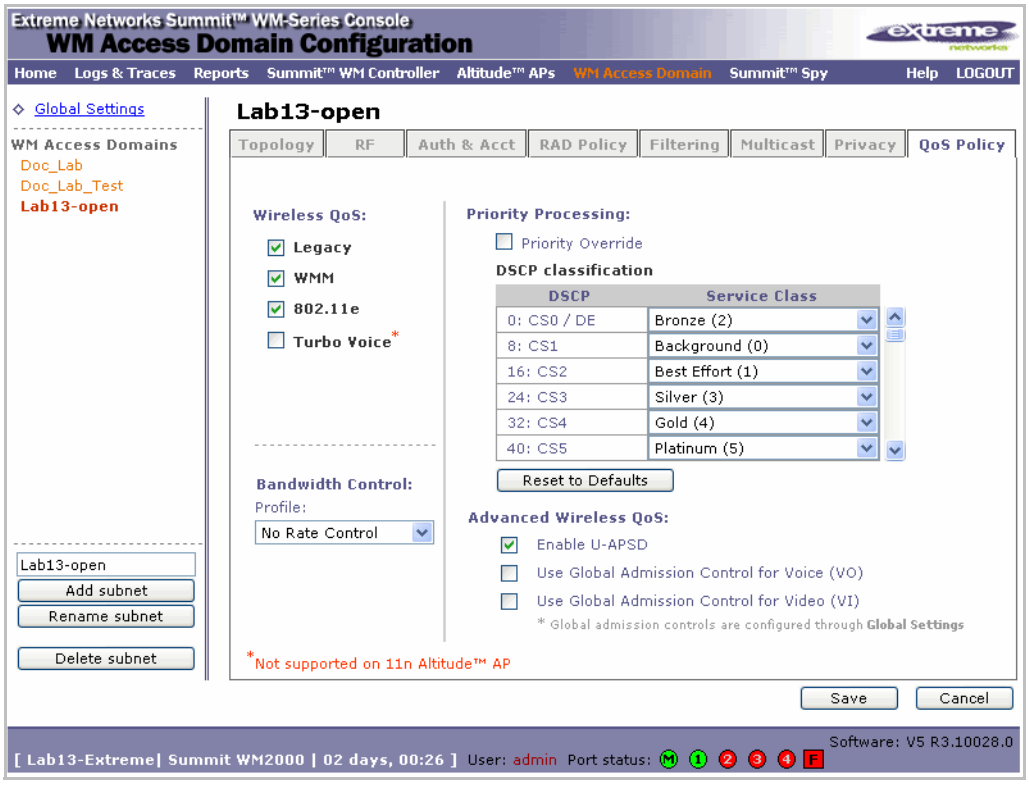
- Select the Bandwidth Control Profile that you want to apply to the WM-AD. The Bandwidth Control Profiles ensure that no single user on any WM-AD is able to consume disproportionate amount of bandwidth. For more information, see "Creating Bandwidth Control profiles" on page 152.

To configure QoS Policy on a WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the WM-AD you want to configure for QoS.

3 Click the **QoS Policy** tab.



4 From the **Wireless QoS** list, do the following:

- **Legacy** - Select if your WM-AD will support legacy devices that use SpectraLink Voice Protocol (SVP) for prioritizing voice traffic. If selected, the Turbo Voice option is displayed.
- **WMM** - Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all WMM clients. Note that WMM clients will also classify and prioritize the

uplink traffic. WMM is part of the 802.11e standard for QoS. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed.

- **802.11e** - Select to enable the AP to accept WMM client associations, and classify and prioritize the downlink traffic for all 802.11e clients. The 802.11e clients will also classify and prioritize the uplink traffic. If selected, the **Turbo Voice** and the **Advanced Wireless QoS** options are displayed:
- **Turbo Voice** - Select to enable all downlink traffic that is classified to the Voice (VO) AC and belongs to that WM-AD to be transmitted by the AP via a queue called Turbo Voice (TVO) instead of the normal Voice (VO) queue. When **Turbo Voice** is enabled together with **WMM** or **802.11e**, the WMM and/or 802.11e clients in that WM-AD are instructed by the AP to transmit all traffic classified to VO AC with special contention parameters tailored to maximize voice performance and capacity.

5 To define the service class and DSCP marking for the WM-AD, select the **Priority Override** checkbox. For each DSCP you can click one of the eight service classes.

- **Service class** - From the drop-down list, click the appropriate priority level:
  - Network control (7) - The highest priority level.
  - Premium (Voice) (6)
  - Platinum (5)
  - Gold (4)
  - Silver (3)
  - Bronze (2)
  - Best Effort (1)
  - Background (0) - The lowest priority level
- **DSCP marking** - From the drop-down list, click the DSCP value used to tag the IP header of the encapsulated packets.

6 If you want to assign a service class to each DSCP marking, clear the **Priority Override** checkbox and define the DSCP service class priorities in the DSCP classification table.

When **Priority Override** is enabled, the configured service class overrides queue selection in the downlink direction, the 802.1P user priority for the VLAN tagged Ethernet packets and the user priority for the wireless QoS packets (WMM or 802.11e), according to the mapping between service class and user priority. If **Priority Override** is enabled and the WM-AD is not locally bridged, the configured DSCP value is used to tag the IP header of the encapsulated packets. The AP does not override the DSCP in the IP header of the user packet.

7 The **Advanced Wireless QoS** options are only displayed if the WMM or 802.11e checkboxes are selected:

- **Enable U-APSD** - Select to enable the Unscheduled Automatic Power Save Delivery (U-APSD) feature. This feature can be used by mobile devices to efficiently sustain one or more real-time streams while being in power-save mode. This feature works in conjunction with WMM and/or 802.11e, and it is automatically disabled if both WMM and 802.11e are disabled.
- **Use Global Admission Control for Voice (VO)** - Select to enable admission control for Voice. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.
- **Use Global Admission Control for Video (VI)** - This feature is only available If admission control is enabled for Voice. Select to enable admission control for Video. With admission control, clients are forced to request admission in order to use the high priority access categories in both downlink and uplink direction. Admission control protects admitted traffic against new bandwidth demands.

- **UL Policer Action** - If **Use Global Admission Control for Voice (VO)** or **Use Global Admission Control for Video (VI)** is enabled, click the action you want the Altitude AP to take when TSPEC violations occurring on the uplink direction are discovered:
  - **Do nothing** - Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.
  - **Send DELTS to Client** - Click to end TSPEC violations when it they are discovered. This action deletes the TSPEC.
- **DL Policer Action** - If **Use Global Admission Control for Voice (VO)** or **Use Global Admission Control for Video (VI)** is enabled, click the action you want the Altitude AP to take when TSPEC violations occurring on the downlink direction are discovered:
  - **Do nothing** - Click to allow TSPEC violations to continue when they are discovered. Data transmissions will continue and no action is taken against the violating transmissions.
  - **Downgrade** - Click to force the transmission's data packets to be downgraded to the next priority when a TSPEC violation is discovered.
  - **Drop** - Click to force the transmission's data packets to be dropped when a TSPEC violation is discovered.

8 To apply the **Bandwidth Control Profile** to the WM-AD, select the profile from the **Bandwidth Control Profile** menu.

9 To save your changes, click **Save**.

Bridging traffic locally

A WM-AD must first be setup before traffic can be bridged locally. For more information, see Chapter 4, "WM Access Domain Services."

To bridge traffic locally:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

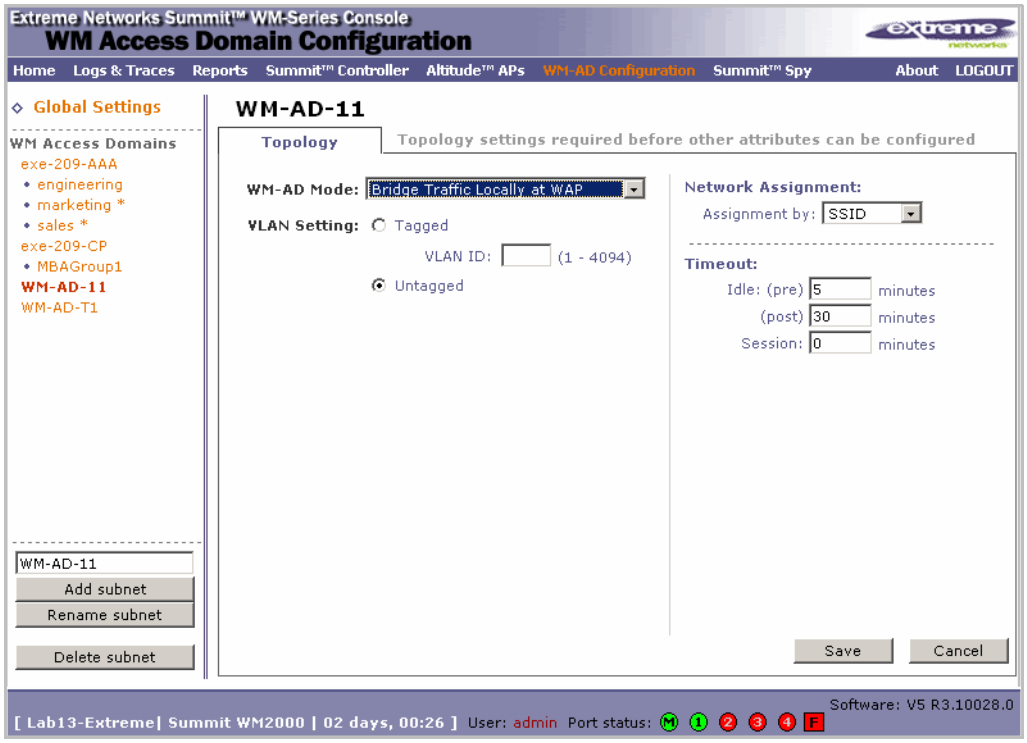
2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box.

3 Click **Add subnet**. The name is displayed in the **WM Access Domain** list. The **Topology** tab is displayed.

4 In the **WM-AD Mode** drop-down list, click **Bridge Traffic Locally at AP** to enable branch office mode.

5 To define the VLAN Setting, select one of the following:
- **Tagged**
- **Untagged**

If you select **Tagged**, type the VLAN ID in the **VLAN ID** box.



NOTE

The VLAN IDs are assigned by the branch office network administrator. The AP will operate correctly if you set the VLAN ID corresponding to the VLAN ID that was setup in the LAN.
Configuring two untagged branch WM-ADs to the same AP on different radios is permitted. This is similar to having two untagged branch WM-ADs with the same VLAN ID assigned to the same AP on different radios. In both cases, the AP will connect the two WM-ADs. That type of configuration can be viewed as a single WM-AD/VLAN with different SSIDs on different radios.
An effective scenario of the configuration described above, in which the same subnet is used with different SSIDs on radio a and b/g, is when this configuration is defined consistently on all APs. It would allow dual band a+b/g clients to associate to one of the radios by specifying the correct SSID. This is particularly effective with Microsoft clients that do not allow defining a preferred radio.

6 To save your changes, click **Save**.

NOTE

In previous releases, an entire AP had to be put into branch mode. In the current release, an individual WM-AD can be put into bridging mode. An AP can have bridged and non-bridged WM-ADs.
If it has more than one branch mode WM-AD, only one bridged WM-AD can be untagged per AP per radio. The other branch mode WM-ADs need to have unique VLAN ID. You must have VLAN aware L2 switches to support this feature.

NOTE

When a WM-AD is setup for bridged mode, it cannot be switched to tunneled mode. The administrator must delete and re-add the WM-AD.

Wireless Distribution System

A Wireless Distribution System (WDS) enables you to expand the wireless network by interconnecting the Altitude APs through wireless links in addition to the traditional method of interconnecting Altitude APs via a wired esnetwork.

NOTE

The Scalance AP W788-2 does not support WDS.

A WDS deployment is ideally suited for locations, where installing ethernet cabling is too expensive, or physically impossible.

The WDS can be deployed in three configurations:

- Simple WDS Configuration
- Wireless Repeater Configuration
- Wireless Bridge Configuration

Simple WDS configuration

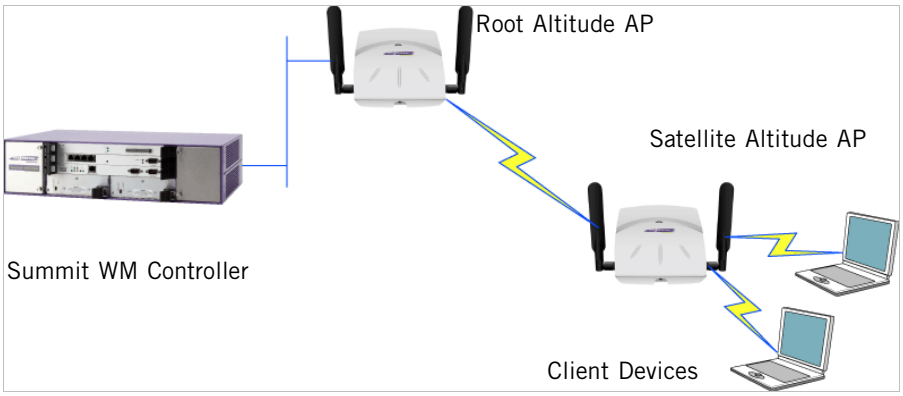
In a typical configuration, the Altitude APs are connected to the distribution system via an Ethernet network, which provides connectivity to the Summit WM Controller.

However, when an Altitude AP is installed in a remote location and can't be wired to the distribution system, an intermediate Altitude AP is connected to the distribution system via the Ethernet link. This intermediate Altitude AP forwards and receives the user traffic from the remote Altitude AP over a radio link.

The intermediate Altitude AP that is connected to the distribution system via the Ethernet network is called Root AP, and the Altitude AP that is remotely located is called the Satellite AP.

The following figure illustrates the Simple WDS configuration:

Figure 10: Simple WDS configuration

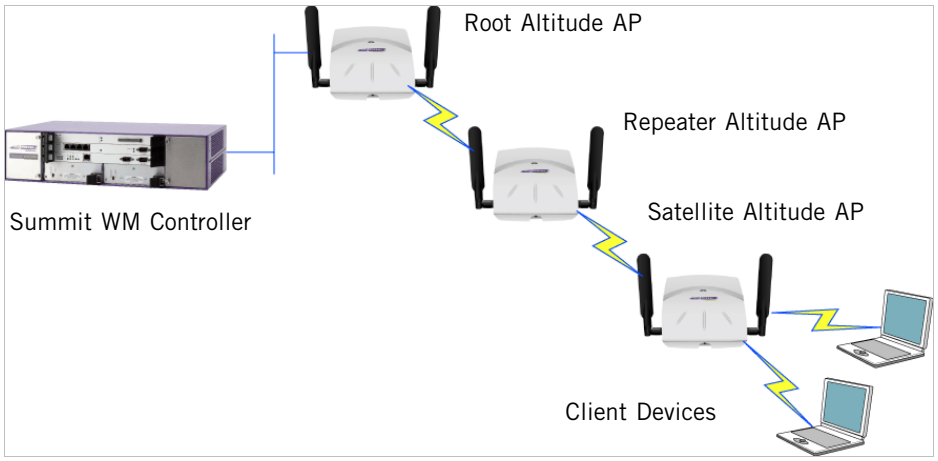


Wireless Repeater configuration

In Wireless Repeater configuration, a Repeater Altitude AP is installed between the Root Altitude AP and the Satellite Altitude AP. The Repeater Altitude AP relays the user traffic between the Root Altitude AP and the Satellite Altitude AP. This increases the WLAN range.

The following figure illustrates the Wireless Repeater configuration:

Figure 11: Wireless Repeater configuration



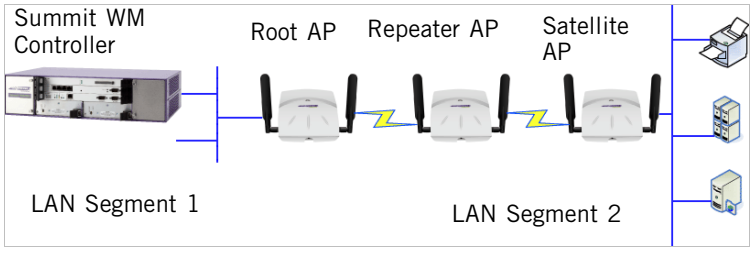
NOTE

You should restrict the number of repeater hops in a Wireless Repeater configuration to three for optimum performance.

Wireless Bridge configuration

In Wireless Bridge configuration, the traffic between two Altitude APs that are connected to two separate wired LAN segments is bridged via WDS link. You may also install a Repeater Altitude AP between the two Altitude APs connected to two separate LAN segments.

Figure 12: Wireless Bridge configuration

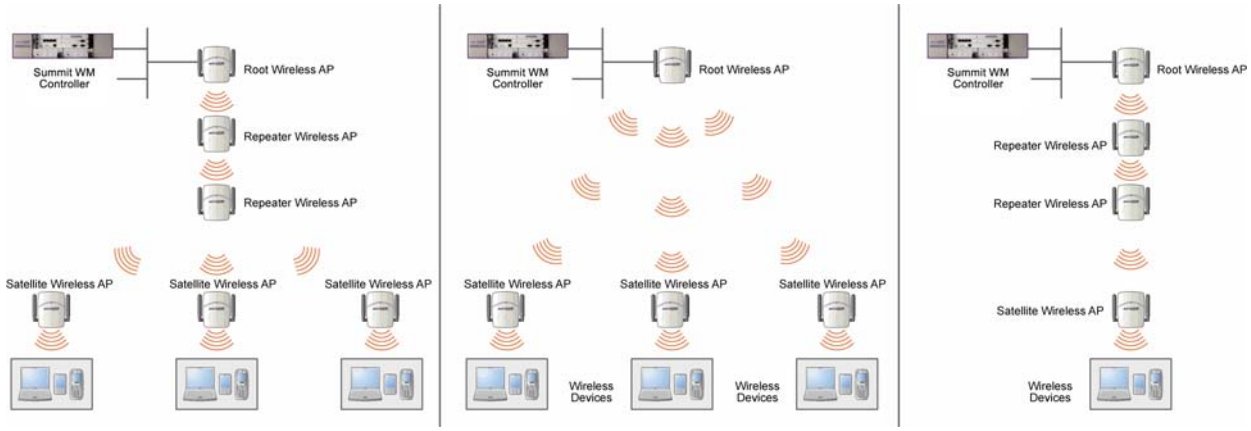


When you are configuring the Wireless Bridge configuration, you must specify on the user interface that the Satellite AP is connected to the wired LAN.

Examples of deployment

The following illustration depicts a few examples of WDS deployment.

Figure 13: Examples of WDS deployment



WDS WM-AD

In a traditional Summit WLAN deployment, each radio of the Altitude AP can interact with the client devices on a maximum of eight network WM-ADs.

In WDS deployment, one of the radios of every WDS Altitude AP establishes a WDS link on an exclusive WM-AD. The WDS Altitude AP is therefore limited to seven network WM-ADs on the WDS radio. The other radio can interact with the client-devices on a maximum of eight WM-ADs.

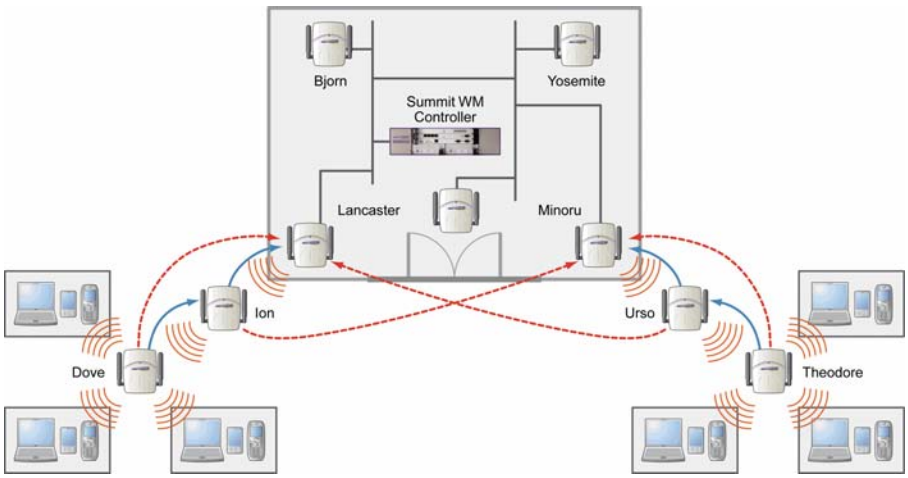
NOTE

The Root Altitude AP and the Repeater Altitude APs can also be configured to interact with the client-devices. For more information, see "Assigning the Satellite Altitude APs' radios to the network WM-ADs" on page 228.

The WM-AD on which the Altitude APs establish the WDS link is called the WDS WM-AD.

A WDS can be setup either by using either a single WDS WM-AD or multiple WDS WM-ADs. The following figures illustrate the point.

Figure 14: Deployment Example

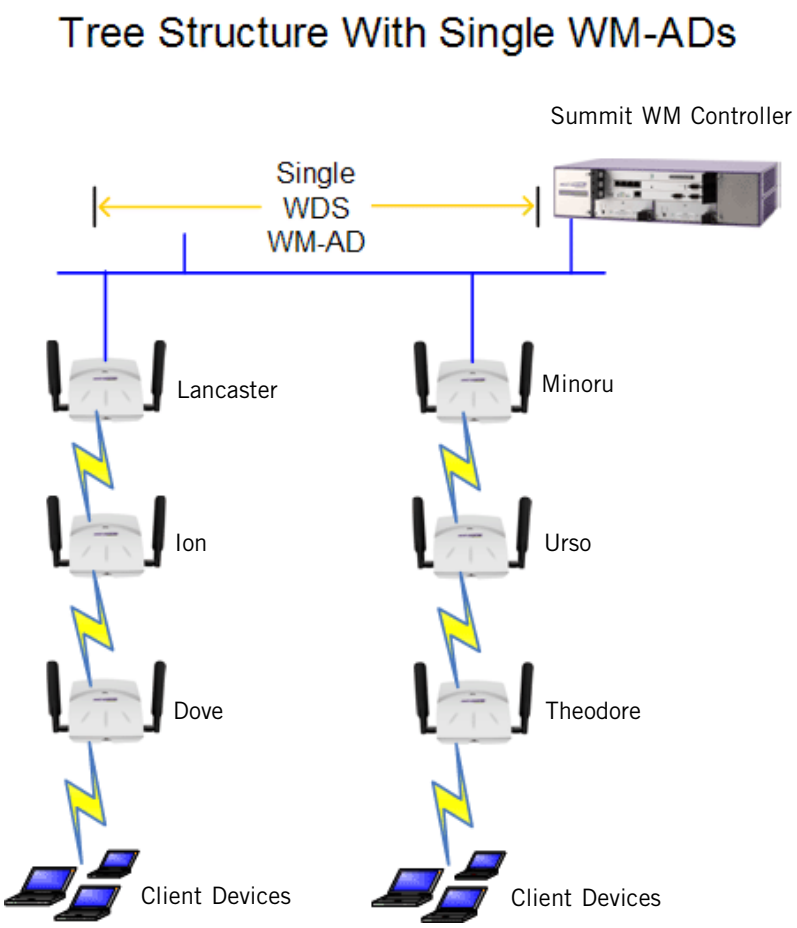


- The rectangular enclosure denotes an office building
- The four Altitude APs - Minoru, Yosemite, Bjorn and Lancaster - are within the confines of the building and are connected to the wired network.
- The space around the office building is a ware house.
- The solid arrows point towards Preferred Parents.
- The dotted arrows point towards Backup Parents.

WDS setup with a single WDS WM-AD

Deploying the WDS for the above example using a single WDS WM-AD results in the following structure.

Figure 15: WDS setup with a single WDS WM-AD

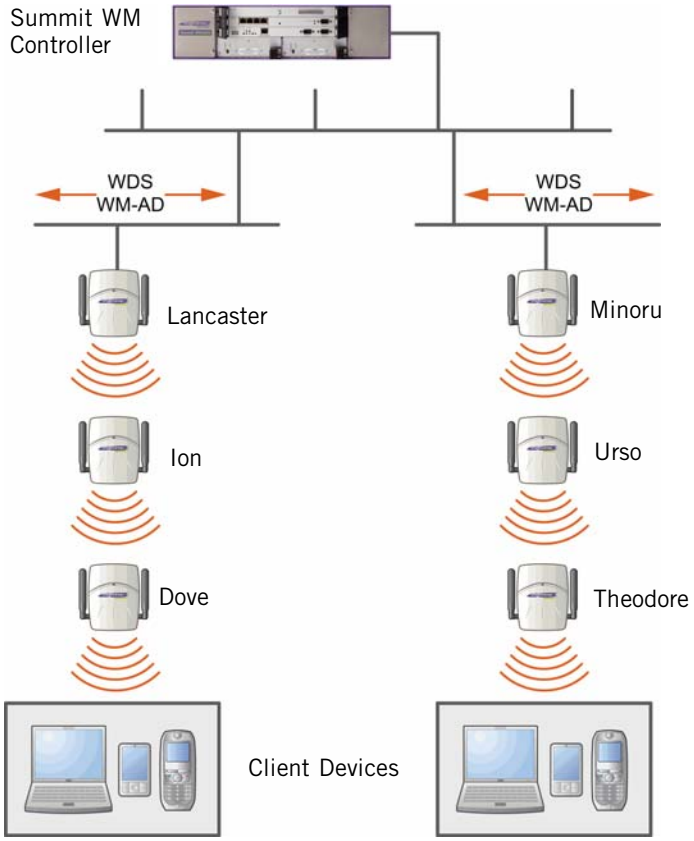


The tree will operate as a single WDS entity. It will have a single WDS SSID and a single pre-shared key for WDS links. This tree will have multiple roots. For more information, see "Multi-root WDS topology" on page 219.

WDS setup with multiple WDS WM-ADs

You can also deploy the same WDS in Figure 14 using two WDS WM-ADs. The Two WDS WM-ADs will create two independent WDS trees. Both the trees will operate on separate SSIDs and use separate pre-shared keys.

Figure 16: WDS setup with multiple WDS WM-ADs



Key features of WDS

Some key features of WDS are:

- Tree-like topology
- Radio Channels
- Multi-root WDS topology
- Automatic discovery of parent and backup parent Altitude APs
- Link security

Tree-like topology

The Altitude APs in WDS configuration can be regarded as nodes, and these nodes form a tree-like structure. The tree builds in a top down manner with the Root Altitude AP being the tree root, and the Satellite Altitude AP being the tree leaves.

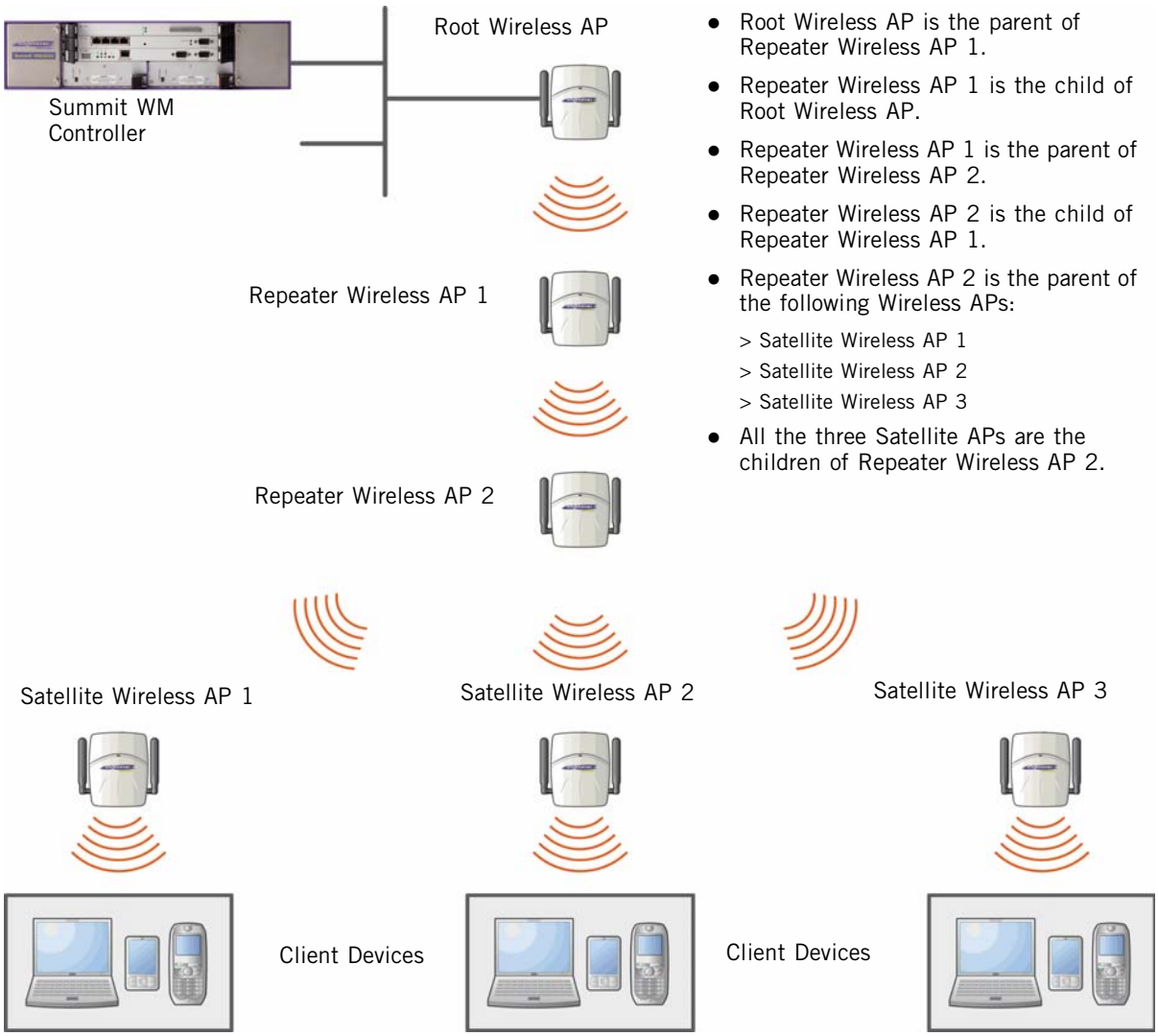
The nodes in the tree-structure have a parent-child relationship. The Altitude AP that provides the WDS service to the other Altitude APs in the downstream direction is a parent. The Altitude APs that establish a link with the Altitude AP in the upstream direction for WDS service are children.

NOTE

If a parent Altitude AP fails or stops to act a parent, the children Altitude APs will attempt to discover their backup parents. If the backup parents are not defined, the children Altitude APs will be left stranded.

The following figure illustrates the parent-child relationship between the nodes in a WDS topology.

Figure 17: Parent-child relationship between Altitude APs in WDS configuration


Root Wireless AP
Summit WM Controller
Repeater Wireless AP 1
Repeater Wireless AP 2
Satellite Wireless AP 1
Satellite Wireless AP 2
Satellite Wireless AP 3
Client Devices
Client Devices
Root Wireless AP is the parent of Repeater Wireless AP 1.
Repeater Wireless AP 1 is the child of Root Wireless AP.
Repeater Wireless AP 1 is the parent of Repeater Wireless AP 2.
Repeater Wireless AP 2 is the child of Repeater Wireless AP 1.
Repeater Wireless AP 2 is the parent of the following Wireless APs:
> Satellite Wireless AP 1
> Satellite Wireless AP 2
> Satellite Wireless AP 3
All the three Satellite APs are the children of Repeater Wireless AP 2.

The WDS system enables you to configure the Altitude AP's role - **parent**, **child** or **both** - from the Summit WM Controller's interface. If the WDS Altitude AP will be serving as a parent and a child in a given topology, its role is configured as **both**.

NOTE

It is recommended to limit the number of APs participating in a WDS tree to 8. This limit guarantees decent performance in most typical situations.

NOTE

If an Altitude AP is configured to serve as a scanner in Summit WM series Spy, it cannot be used in a WDS tree. For more information, see Chapter 9, "Working with the Summit WM series Spy."

Radio Channels

The radio channel on which the child Altitude AP operates is determined by the parent Altitude AP.

An Altitude AP may connect to its parent Altitude AP and children Altitude APs on the same radio, or on different radios. Similarly, an Altitude AP can have two children operating on two different radios.

NOTE

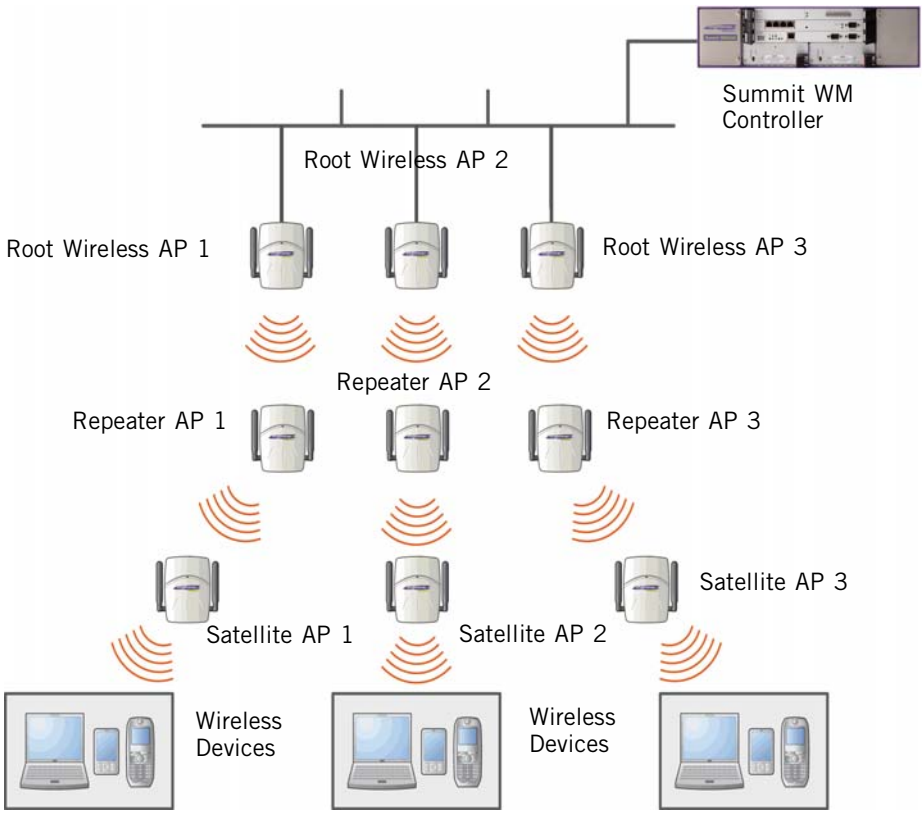
When an Altitude AP is connecting to its parent Altitude AP and children APs on the same radio, it uses the same channel for both the connections.

Multi-root WDS topology

A WDS topology can have multiple Root Altitude APs.

Figure 18 illustrates the multiple-root WDS topology.

Figure 18: Multiple-root WDS topology



Automatic discovery of parent and backup parent Altitude APs

The children Altitude APs, including the Repeater Altitude AP and the Satellite Altitude APs, scan for their respective parents at a startup.

You can configure a parent and backup parent for the children Altitude APs. The Altitude APs will first try to negotiate a WDS link with the parent Altitude AP. If the WDS link negotiation is unsuccessful, the Altitude AP will try to negotiate a link with the backup parent.

Link security

The WDS link is encrypted using Advance Encryption Standard (AES).

NOTE

The keys for AES are configured prior to deploying the Repeater or Satellite Altitude APs.

Deploying the WDS system

Before you start configuring the WDS Altitude APs, you must ensure the following:

- The Altitude APs that are part of the wired Summit WLAN are connected to the wired network.

- The wired Altitude APs that will serve as the Root AP/Root APs of the proposed WDS topology are operating normally.
- The Summit WLAN is operating normally.

Sketching the WDS topology

You may sketch the proposed WLAN topology on a paper before you start the WDS deployment process. You should clearly identify the following in the sketch:

- WDS Altitude APs with their names
- Parent-Child relationships between Altitude APs
- Radios that you will choose to link the Altitude AP's parents and children

Provisioning the WDS Altitude APs

This step is of crucial importance and involves connecting the WDS Altitude APs to the enterprise network via the Ethernet link. This is done to enable the WDS Altitude APs to connect to the Summit WM Controller so that they can derive their WDS configuration.

The WDS Altitude AP's configuration includes pre-shared key, its role, preferred parent name and the backup parent name.

NOTE

The provisioning of WDS Altitude APs must be done before they are deployed at the target location. If the Altitude APs are not provisioned, they will not work at their target location.

WDS deployment overview

The following is the high-level overview of the WDS deployment process:

1 Connecting the WDS Altitude APs to the enterprise network via the Ethernet network to enable them to discover and register themselves with the Summit WM Controller. For more information, see "Discovery and registration overview" on page 71.

2 Disconnecting the WDS Altitude APs from the enterprise network after they have discovered and registered with the Summit WM Controller.

3 Creating a WDS WM-AD.

4 Assigning roles, parents and backup parents to the WDS Altitude APs.

5 Assigning the Satellite Altitude APs' radios to the network WM-ADs.

6 Connecting the WDS Altitude APs to the enterprise network via the Ethernet link for provisioning. For more information, see "Provisioning the WDS Altitude APs" on page 221.

7 Disconnecting the WDS Altitude APs from the enterprise network and moving them to the target location.

NOTE

During the WDS deployment process, the WDS Altitude APs are connected to the enterprise network on two occasions - first to enable them to discover and register with the Summit WM Controller, and then the second time to enable them to obtain the provisioning from the Summit WM Controller.

Connecting the WDS Altitude APs to the enterprise network for discovery and registration

Connect each WDS Altitude AP to the enterprise network to enable it to discover and register themselves with the Summit WM Controller.

NOTE

*Before you connect the **WDS Altitude APs** to the enterprise network for discovery and registration, you must ensure that the **Security mode** property of the Summit WM Controller is defined according to your security needs. The **Security mode** property dictates how the Summit WM Controller behaves when registering new and unknown devices. For more information, see "Defining properties for the discovery process" on page 80.*
*If the **Security mode** is set to **Allow only approved Altitude APs to connect** (this is also known as secure mode), you must manually approve the WDS Altitude APs after they are connected to the network for the discovery and registration. For more information, see "Adding and registering an Altitude AP manually" on page 83.*

Depending upon the number of Ethernet ports available, you may connect one or more WDS Altitude AP at a time, or you may connect all of them together.

Once a WDS Altitude AP has discovered and registered itself with the Summit WM Controller, disconnect it from the enterprise network.

Configuring the WDS Altitude APs through the Summit WM Controller

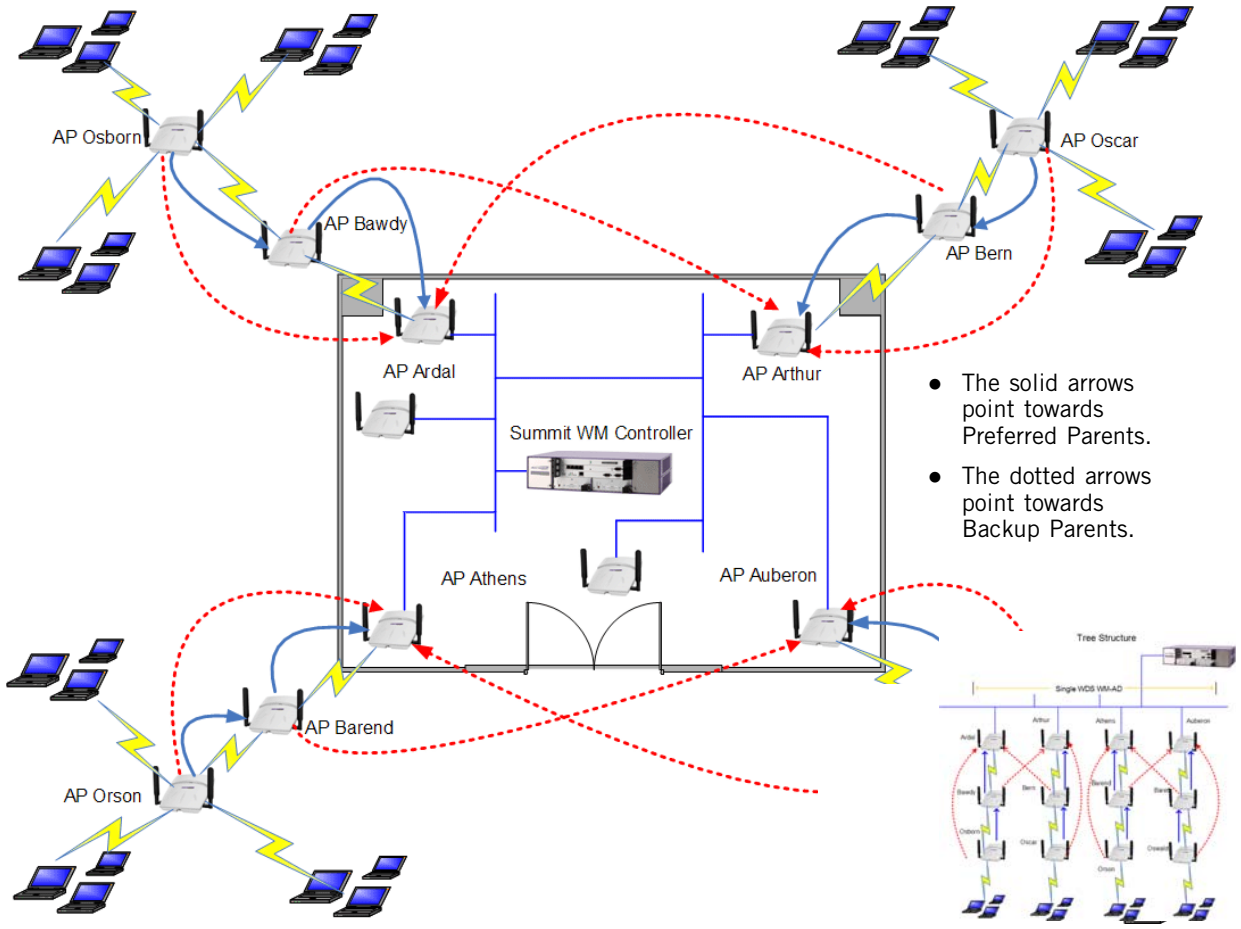
Configuring the WDS Altitude APs involves the following steps:

1. Creating a WDS WM-AD.
2. Defining the SSID name and the pre-shared key.
3. Assigning roles, parents and backup parents to the WDS Altitude APs.

For the ease of understanding, the WDS configuration process is explained with the help of an example. The following illustration depicts a site with the following features:

- An office building, denoted by a rectangular enclosure.
- Four Altitude APs - Ardal, Arthur, Athens and Auberon - are within the confines of the building, and are connected to the wired network.
- The space around the building is the ware house.

Figure 19: WDS Deployment



NOTE

*With the single WDS WM-AD, the tree structure for the WDS deployment will be as depicted on the bottom right of Figure 19. You can also implement the same deployment using four WDS WM-ADs, each for a set of Altitude APs in the four corners of the building. Each set of Altitude APs will form an isolated topology and will operate using a separate **SSID** and a separate **Pre-shared** key. For more information, see "WDS WM-AD" on page 214.*

To configure the WDS Altitude APs through the Summit WM Controller:

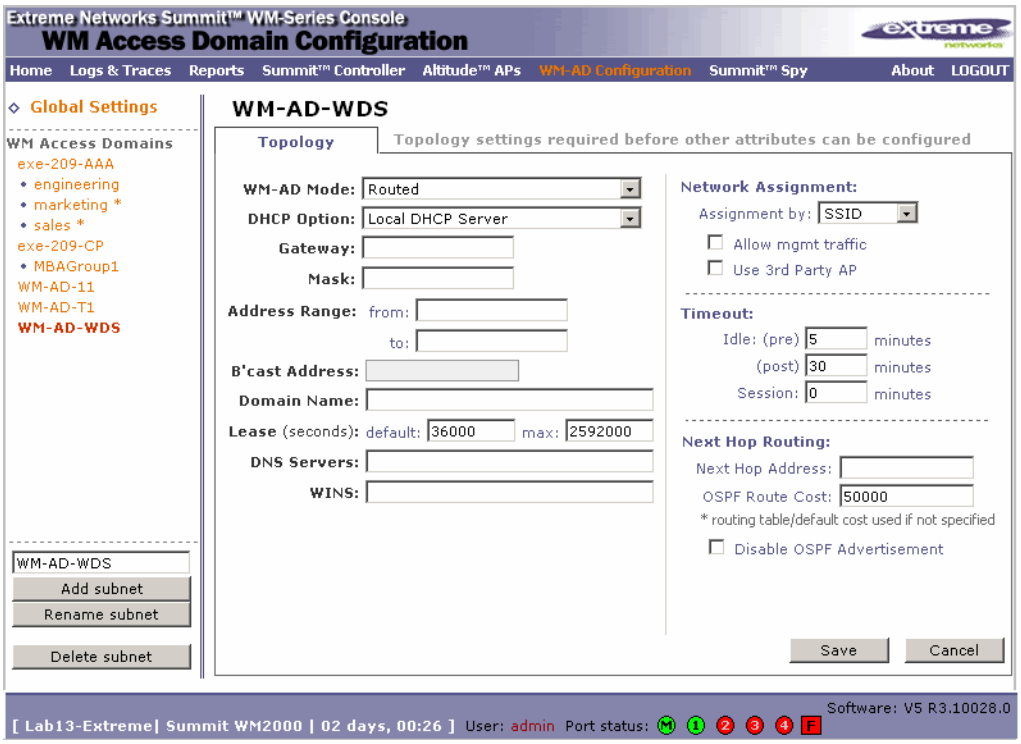
NOTE

You must identify and mark the Preferred Parents, Backup Parents and the Child Altitude APs in the proposed WDS topology before starting the configuration process.

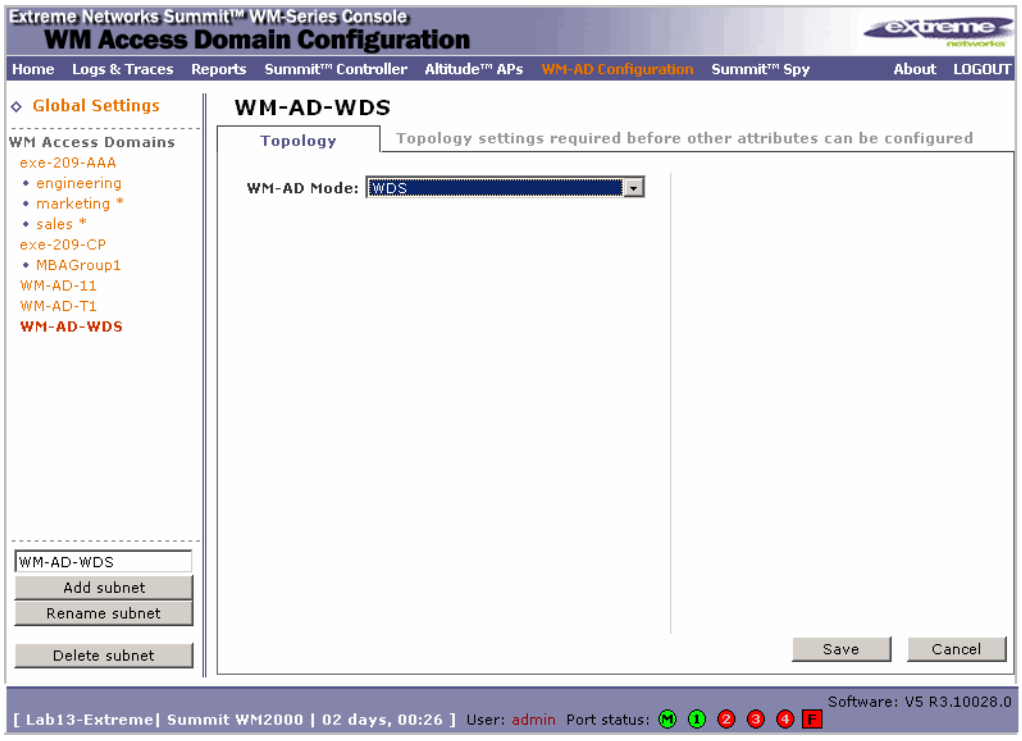
1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane, type the WDS WM-AD name in the **Add subnet** box.

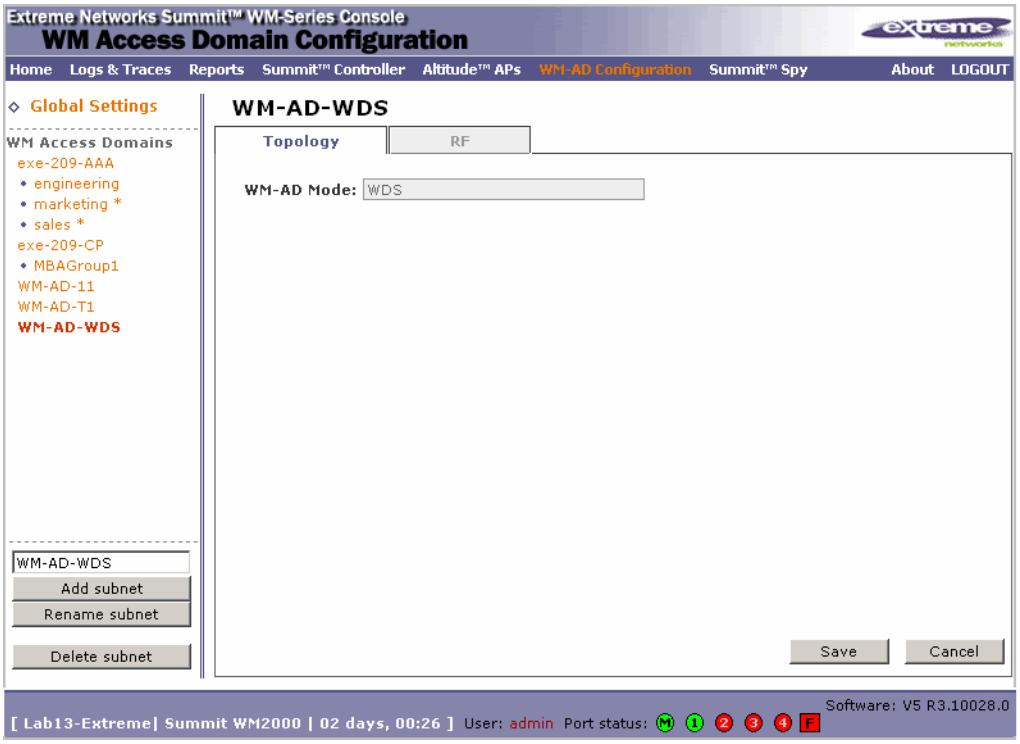
3 Click **Add subnet**. The name is displayed in the WM Access Domains list and the **Topology** tab is displayed.



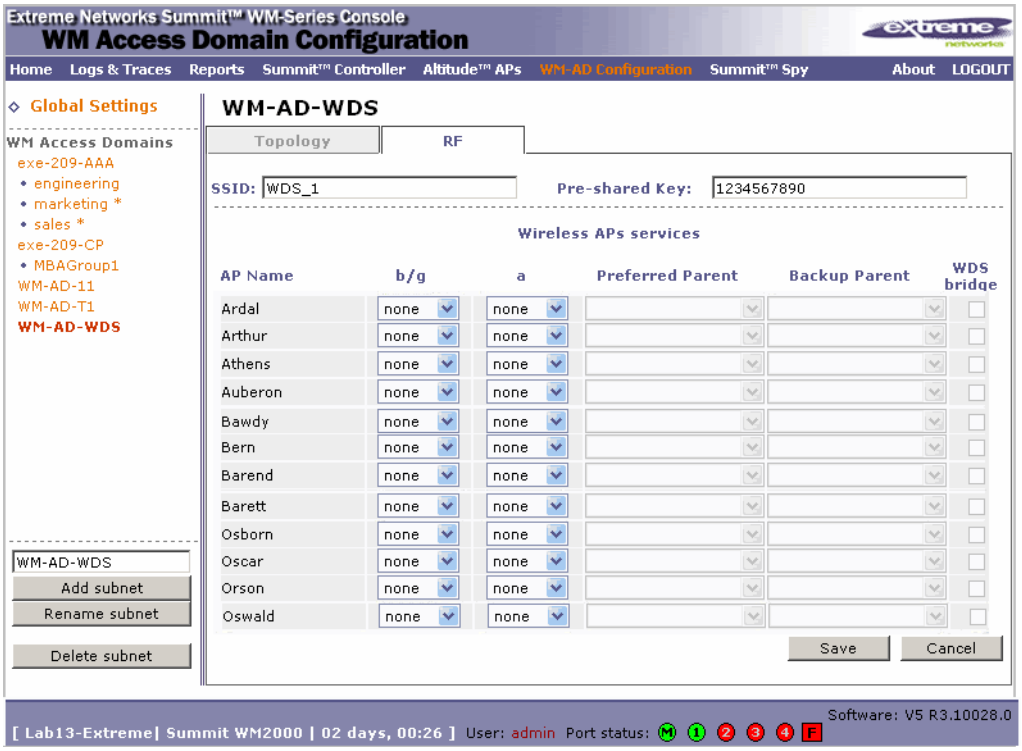
4 From the **WM-AD Mode** drop-down list, click **WDS**. The **WDS Topology** tab is displayed.



5 To save your changes, click **Save**. The **Topology** tab is displayed.



6 Click the **RF** tab.



7 In the **SSID** box, type a name that will identify the new WDS SSID.

8 In the **Pre-shared Key** box, type the key.

NOTE

The pre-shared key must be 8 to 63 characters long.
The WDS Altitude APs use this pre-shared key to establish a WDS link between them.

NOTE

Changing the pre-shared key after the WDS is deployed can be a lengthy process. For more information, see *"Changing the pre-shared key in WDS WM-AD" on page 229*.

9 Assign the roles, preferred parents and backup parents to the Altitude APs.

NOTE

*The roles - **parent**, **child**, and **both** - are assigned to the radios of the Altitude APs. An Altitude AP may connect to its parent Altitude AP and children Altitude APs on the same radio, or on different radios. Similarly, an Altitude AP can have two children operating on two different radios.*
The radio channel on which the child Altitude AP operates is determined by the parent Altitude AP.
*If the Altitude AP will be serving both as parent and child, you must select **both** as its role.*

To configure the WDS as illustrated in Figure 19 with a single WDS WM-AD, you must assign the roles, preferred parents and backup parents to the Altitude APs according to the following table:

Table 27: Altitude APs and their roles

Altitude AP	Radio b/g	Radio a	Preferred Parent	Backup Parent
Ardal	Parent	Parent	See the note below.	See the note below.
Arthur	Parent	Parent	See the note below.	See the note below.
Athens	Parent	Parent	See the note below.	See the note below.
Auberon	Parent	Parent	See the note below.	See the note below.
Bawdy	Both	Child	Ardal	Arthur
Bern	Both	Child	Arthur	Ardal
Barend	Both	Child	Athens	Auberon
Barett	Both	Child	Auberon	Athens
Osborn	Child	Child	Bawdy	Ardal
Oscar	Child	Child	Bern	Arthur
Orson	Child	Child	Barend	Athens
Oswald	Child	Child	Barett	Auberon

NOTE

*Since the Root Altitude APs - Ardal, Arthur, Athens and Auberon - are the highest entities in the tree structure, they do not have parents. Therefore, the **Preferred Parent** and **Backup Parent** drop-down lists of the Root Altitude APs do not display any Altitude AP. You must leave these two fields blank.*

NOTE

*You must first assign the 'parent' role to the Altitude APs that will serve as the parents. Unless this is done, the Parent Altitude APs will not be displayed in the **Preferred Parent** and **Backup Parent** drop-down lists of other Altitude APs.*

NOTE

*The **WDS Bridge** feature on the user interface relates to **WDS Bridge** configuration. When you are configuring the WDS Bridge topology, you must select WDS Bridge for Satellite Altitude AP that is connected to the wired network. For more information, see "Wireless Bridge configuration" on page 213.*

To assign the roles, preferred parent and backup parent:

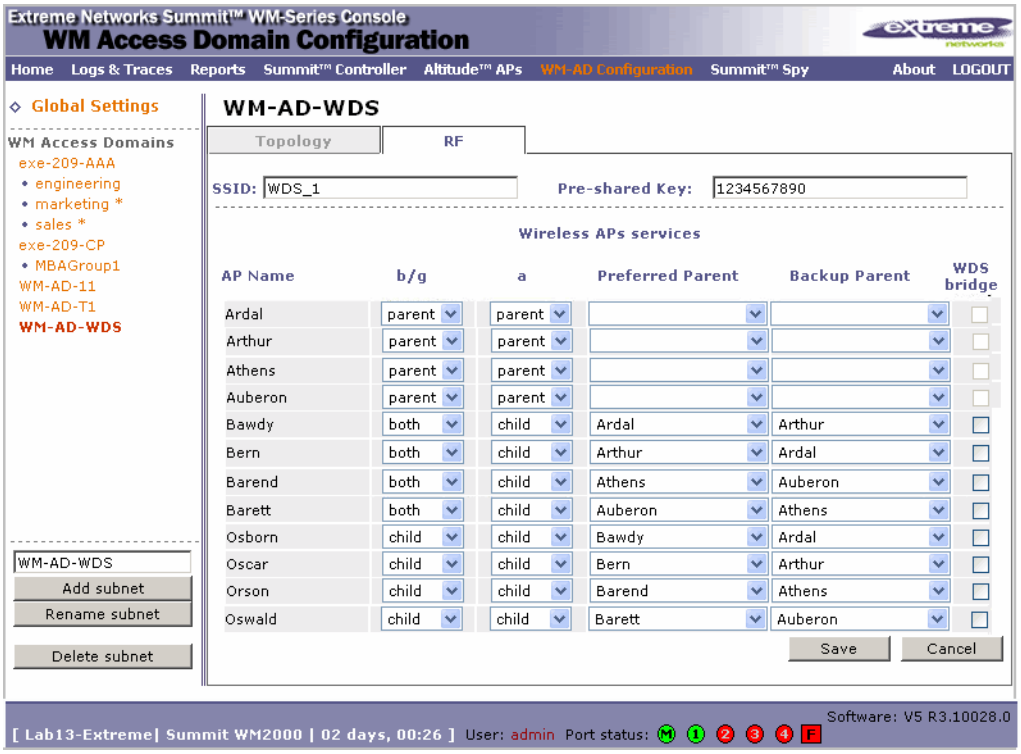
a From the radio **b/g** drop-down list of the Root Altitude APs - Ardal, Arthur, Athens and Auberon, click **Parent**.

b From the radio **a** drop-down list of the Root Altitude APs - Ardal, Arthur, Athens and Auberon, click **Parent.**

c From the radio **a** and radio **b/g** drop-down list of other Altitude APs, click the roles according to Table 27.

d From the **Preferred Parent** drop-down list of other Altitude APs, click the parents according to Table 27.

e From the **Backup Parent** drop-down list of other Altitude APs, click the backup parents according to Table 27.



10 To save your changes, click **Save**.

Assigning the Satellite Altitude APs' radios to the network WM-ADs

You must assign the Satellite Altitude APs's radios to the network WM-ADs.

NOTE

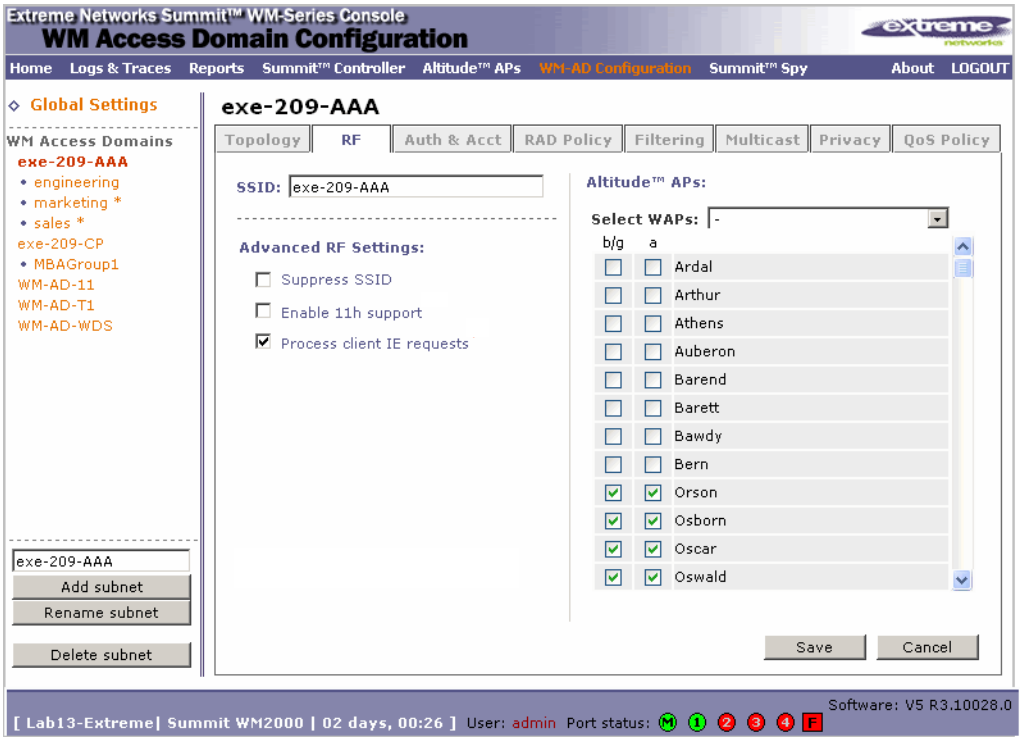
The network WM-ADs are the usual WM-ADs on which the Altitude APs service the client devices. ***Routed, Bridge Traffic Locally at WM*** *and* ***Bridge Traffic Locally at AP WM-ADs*** *are the network WM-ADs. For more information, see* *"WM-AD Types" on page 156**.*

To assign the Satellite Altitude APs' radios to the network WM-AD:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane **WM Access Domains** list, click the network WM-AD that you want to assign to the radios of Satellite Altitude APs.

3 Click the **RF** tab.



4 In the **Altitude APs** list, select the radios of the Satellite APs - Osborn, Oscar, Orson and Oswald.

NOTE

If you want the Root Altitude AP and the Repeater Altitude APs to service the client devices, you must select their radios in addition to the radios of the Satellite Altitude APs.

5 To save your changes, click **Save**.

6 Log out from the Summit WM Controller.

Connecting the WDS Altitude APs to the enterprise network for provisioning

You must connect the WDS Altitude APs to the enterprise network once more in order to enable them to obtain their configuration from the Summit WM Controller. The configuration includes the pre-shared key, the Altitude AP's role, preferred parent and backup parent. For more information, see "Provisioning the WDS Altitude APs" on page 221.

WARNING!

If you skip this step, the WDS Altitude APs will not work at their target location.

Moving the WDS Altitude APs to the target location

1 Disconnect the WDS Altitude APs from the enterprise network, and move them to the target location.

2 Install the WDS Altitude APs at the target location.

3 Connect the Altitude APs to a power source. The discovery and registration processes are initiated.

NOTE

If you change any of the following configuration parameters of a WDS Altitude AP, the WDS Altitude AP will reject the change:
*- Reassigning the WDS Altitude AP's role from **Child** to **None***
*- Reassigning the WDS Altitude AP's role from **Both** to **Parent***
*- Changing the **Preferred Parent** of the WDS Altitude AP*
However, the Summit WM Controller will display your changes, as these changes will be saved in the database. To enable the WDS Altitude AP to obtain your changes, you must remove it from the WDS location and then connect it to the Summit WM Controller via the wired network.

NOTE

If you change any of the following radio properties of a WDS Altitude AP, the WDS Altitude AP will reject the change:
- Disabling the radio on which the WDS link is established
- Changing the radio's Tx Power of a radio on which the WDS link is established
- Changing the country

Changing the pre-shared key in WDS WM-AD

To change the pre-shared key in WDS WM-AD:

1 Create a new WDS WM-AD with a new pre-shared key.

2 Assign the RF of the Altitude APs from the old WDS to the new WDS WM-AD.

3 Check the **WDS Wireless AP Statistics** report page to ensure that all the WDS Altitude APs have connected to the Summit WM Controller via the new WDS WM-AD. For more information, see "Viewing statistics for Wireless APs" on page 277.

4 Delete the old WDS WM-AD. For more information, see "Deleting a WM-AD" on page 166.

6 Availability and session availability

This chapter describes the availability feature, including:

- "Availability" on page 231
- "Session availability" on page 237
- "Viewing the Altitude AP availability display" on page 251
- "Viewing SLP activity" on page 251

Availability

The Summit WM Software system provides the "availability" feature to maintain service availability in the event of a Summit WM Controller outage.

The availability feature links two Summit WM Controllers - the primary controller and the secondary controller (backup controller). The primary and the secondary controllers share information about their Altitude APs. If the primary controller fails, its Altitude APs failover to the secondary controller. The secondary controller provides the wireless network and a pre-assigned WM-ADs for the Altitude APs.

NOTE

During the failover event, the maximum number of failover APs the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform.

NOTE

Altitude APs that attempt to connect to the secondary controller during a failover event are assigned to the WM-AD that is defined in the system's default AP configuration, provided the administrator has not assigned the failover Altitude APs to one or more WM-ADs. If a system default AP configuration does not exist for the controller (and the administrator has not assigned the failover Altitude APs to any WM-AD), the APs will not be assigned to any WM-AD during the failover. A Summit WM Controller will not accept a connection by a foreign AP if the Summit WM Controller believes its availability partner controller is in service. Also, the default Altitude AP configuration assignment is only applicable to new APs that failover to the backup controller. Any Altitude AP that has previously failed over and is already known to the backup system will receive the configuration already present on that system. For more information, see "Configuring the default Altitude AP settings" on page 125

During the failover event when the Altitude AP connects to the secondary controller, the users are disassociated with the Altitude AP. Consequently, the users must log on again and be authenticated on the secondary controller before the wireless service is restored.

NOTE

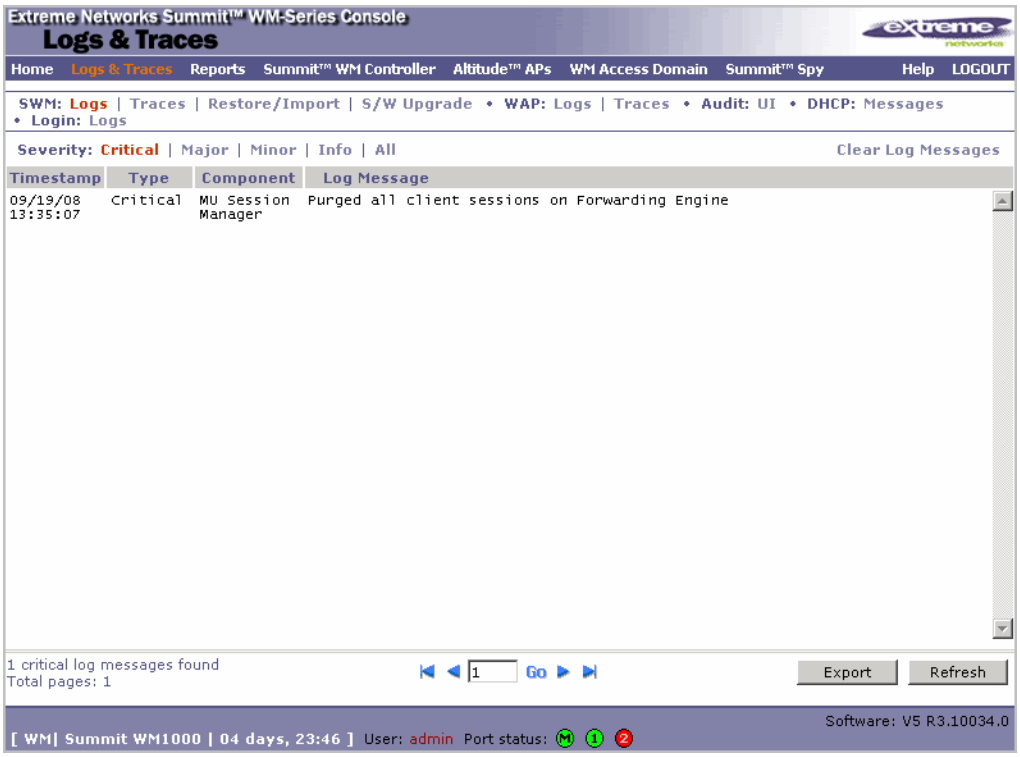
If you want the user session to be maintained, you must use the 'session availability' feature that enables the primary controller's Altitude APs to failover to the secondary controller fast enough to maintain the session availability (user session). For more information, "Session availability" on page 237.

NOTE

The availability feature provides Altitude APs with a list of interfaces. The Altitude AP should attempt to connect automatically to these interfaces when the connection with an active controller link is lost. The provided list identifies the local active interfaces (enabled on the primary and backup controllers) for the active controller as well as the active interfaces for the backup controller. The list is sorted by top-down priority. If the active link is lost (poll failure), the Altitude AP automatically scans (pings) all addresses in its availability interface list. The Altitude AP will then connect to the highest priority interface that responds to its probe.

Events and actions in availability

If one of the Summit WM Controllers in a pair fails, the connection between the two Summit WM Controllers is lost. This triggers a failover condition following which a critical message is displayed in the information log of the secondary Summit WM Controller.



After the Altitude AP on the failed Summit WM Controller loses its connection, it will try to connect to all enabled interfaces on both controllers without rebooting. If the Altitude AP is successful, it will begin the discovery process. If the Altitude AP is not successful in connecting to the Summit WM Controller after five minutes of attempting, the Altitude AP will reboot.

If the Altitude AP is assigned to different WM-ADs on the two controllers, it will reboot. Because of the pairing of the two Summit WM Controllers, the Altitude AP will then register with the other Summit WM Controller.

All user sessions using the failover Altitude AP will terminate unless the **Maintain client sessions in event of poll failure** option is enabled on the **AP Properties** tab or **AP Default Settings** page.

When the Altitude APs connect to the second Summit WM Controller, they are assigned to the WM-AD that is defined in the system's default AP configuration. The wireless device users log on again and are authenticated on the second Summit WM Controller.

When the failed Summit WM Controller recovers, each Summit WM Controller in the pair goes back to normal mode. They exchange information includes the latest lists of registered Altitude APs. The administrator must release the Altitude APs manually on the second Summit WM Controller, so that they may re-register with their home Summit WM Controller. Foreign APs can now all be released at once by using the **Foreign** button on the **Access Approval** page to select all foreign APs, and then clicking **Release**.

To support the availability feature during a failover event, administrators need to do the following:

1 Monitor the critical messages for the failover mode message, in the information log of the remaining Summit WM Controller (in the **Reports and Displays** section of the Summit WM Controller).

2 After recovery, on the Summit WM Controller that did not fail, select the foreign Altitude APs, and then click **Release** on the **Access Approval** page.

Availability prerequisites

Before you begin, ensure you have completed the following:

- Choose the primary and secondary Summit WM Controllers.
- Verify the network accessibility for the UDP connection between the two controllers. The availability link is established as a UDP session on port 13911.
- Set up a DHCP server for AP subnets to support Option 78 for SLP, so that it points to the IP addresses of the physical interfaces on both the Summit WM Controllers.

NOTE

You must ensure that the Poll Timeout value on the AP Properties page is set to 1.5 to 2 times of Detect link failure value on Altitude AP Registration page. For more information, see "Modifying an Altitude AP's properties" on page 86.

If the Poll Timeout value is less than 1.5 to 2 times of Detect link failure value, the Altitude AP failover will not succeed because the secondary controller will not be 'ready' to accept the failover APs.

On the other hand, if the Poll Timeout value is more than 1.5 to 2 times of Detect link failure value, the Altitude APs failover will be unnecessarily delayed, because the Altitude APs will continue polling the primary controller even though the secondary controller is "ready" to accept them as the failover APs.

In order to achieve ideal 'availability' behavior, you must set the Poll Timeout value on the AP Registration page to 15 seconds, and the Detect link failure on Altitude AP Registration page to nine seconds.

Now set up each Summit WM Controller separately. One method is as follows:

1 On the **AP Registration** page, set up each Summit WM Controller in Stand-alone Mode.

2 On the **Topology** tab, define a WM-AD on each Summit WM Controller with the same SSID. The IP addresses must be unique. For more information, see "Topology of a WM-AD" on page 143. A Summit WM Controller WM20/200/2000 VLAN Bridged WM-AD can permit two controllers to share the same subnet (different IP addresses). This setup provides support for mobility users in a VLAN Bridged WM-AD.

3 On both Summit WM Controllers, set the Registration Mode to **Allow only approved** so that no more Altitude APs can register unless they are approved by the administrator.

4 On the **AP Registration** page, enable the two Summit WM Controllers as an availability pair.

5 On each Summit WM Controller, on the **Access Approval** page, check the status of the Altitude APs and approve any APs that should be connected to that controller.

System AP defaults can be used to assign a group of WM-ADs to the foreign APs:

- If the APs are not yet known to the system, the AP will be initially configured according to AP default settings. To ensure better transition in availability, it is recommended that the AP default settings match the desired WM-AD assignment for failover APs.
- AP assignment to WM-ADs according to the AP default settings can be overwritten by manually modifying the AP WM-AD assignment. (For example, select and assign each WM-AD that the AP should connect to.)
- If specific foreign APs have been assigned to a WM-AD, those specific foreign AP assignments are used.

An alternate method to setting up APs includes:

1 Add each Altitude AP manually to each Summit WM Controller.

2 On the **AP Properties** page, click **Add Altitude AP**.

3 Define the Altitude AP, and then click Add Altitude AP.

Manually defined APs will inherit the default AP configuration settings.

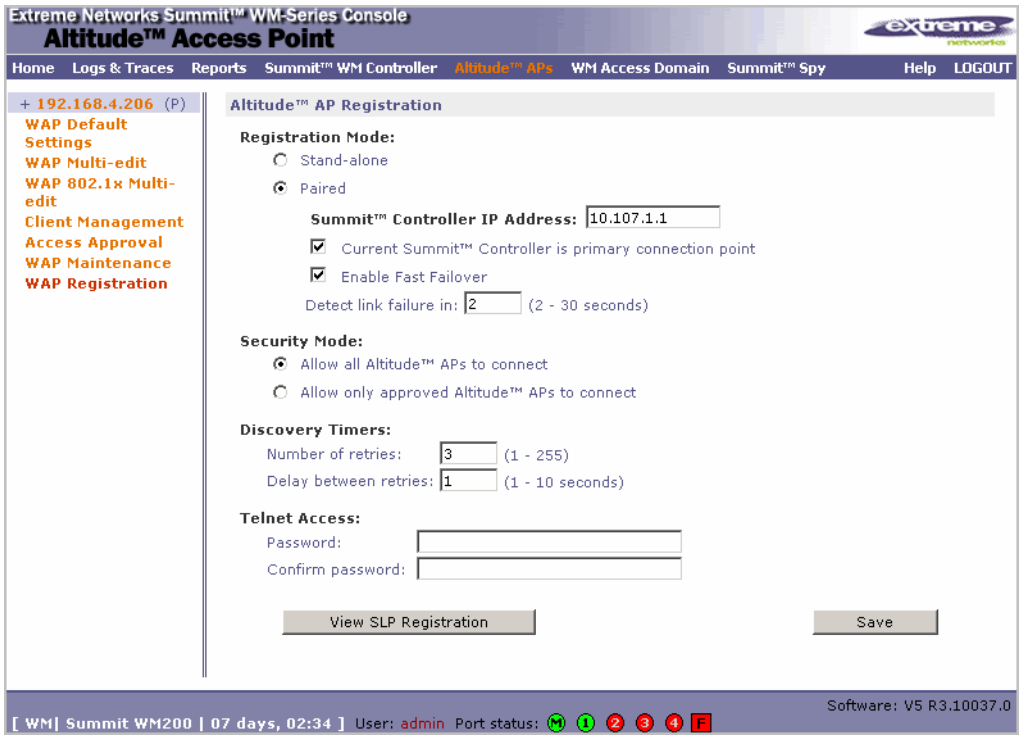
CAUTION

*If two Summit WM Controllers are paired and one has the **Allow All** option set for Altitude AP registration, all APs will register with that Summit WM Controller.*

To set the primary or secondary Summit WM Controllers for availability:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Registration** page is displayed.

2 In the left pane, click **WAP Registration**. The **Altitude AP Registration** page is displayed.



3 To enable availability, select the Paired option.

4 Do one of the following:

- For a primary controller, in the **Summit Controller IP Address** box, type the IP address of the physical port of the secondary Summit WM Controller. This IP address must be on a routable subnet between the two Summit WM Controllers.
- For a secondary controller, in the **Summit Controller IP Address** box, type the IP address of the Management port or physical port of the primary Summit WM Controller.

5 Do one of the following:

- To set this Summit WM Controller as the primary connection point, select the **Current Summit Controller is primary connect poin**t checkbox.
- To set this Summit WM Controller as the secondary connection point, clear the **Current Summit Controller is primary connect point** checkbox.

If the **Current Summit Controller is primary connect point** checkbox is selected, the specified controller waits for a request. If the **Current Summit Controller is primary connect point** checkbox is cleared, the specified controller sends a connection request. Confirm that one controller has this checkbox selected, and the second controller has this checkbox cleared, since improper configuration of this option will result in incorrect network configuration.

6 On both the primary and secondary controllers, type the **Detect link failure value**.

NOTE

*You must ensure that the **Detect link failure** value on both the controllers must be identical.*

7 To set the security mode for the Summit WM Controller, select one of the following options:

- **Allow all Altitude APs to connect** - If the Summit WM Controller does not recognize the serial number, it sends a default configuration to the Altitude AP. Or, if the Summit WM Controller

recognizes the serial number, it sends the specific configuration (port and binding key) set for that Altitude AP.

- **Allow only approved Altitude APs to connect** - If the Summit WM Controller does not recognize the serial number, the operator is prompted to create a configuration. Or, if the Summit WM Controller recognizes the serial number, it sends the configuration for that Altitude AP.

NOTE

*During the initial setup of the network, it is recommended to select the **Allow all Altitude APs to connect** option. This option is the most efficient way to get a large number of Altitude APs registered with the Summit WM Controller.*

*Once the initial setup is complete, it is recommended that the security mode is reset to the **Allow only approved Altitude APs to connect** option. This option ensures that no unapproved Altitude APs are allowed to connect. For more information, see "Configuring Altitude AP settings" on page 84.*

8 To save your changes, click **Save**.

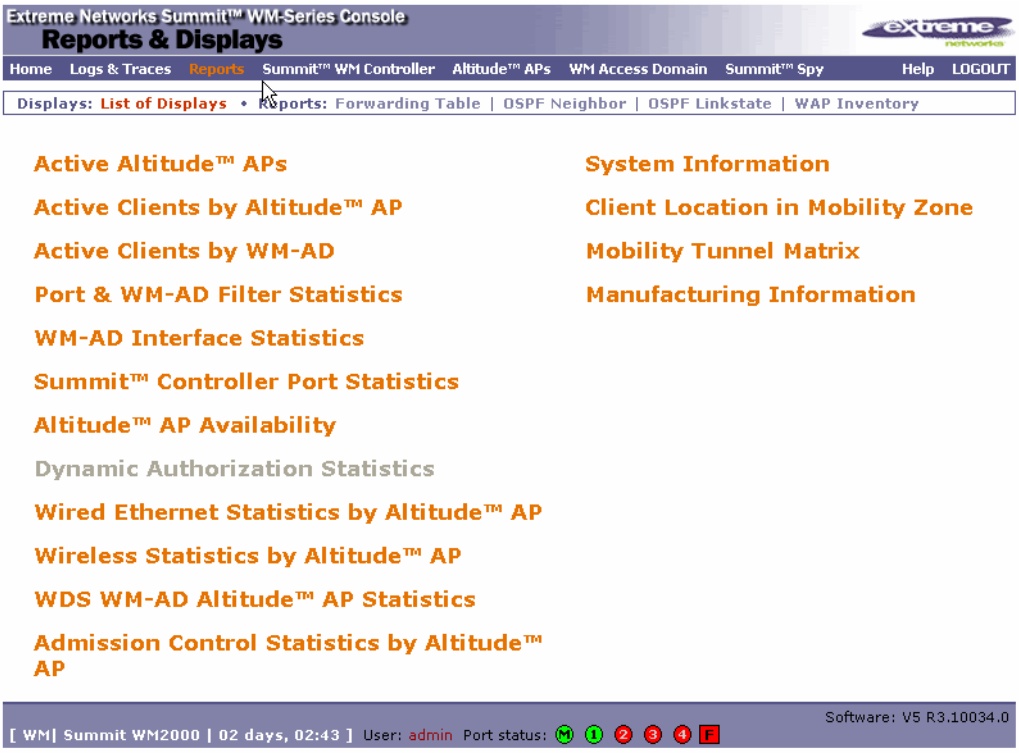
NOTE

When two Summit WM Controllers have been paired as described above, each Summit WM Controller's registered Altitude APs will appear as foreign on the other controller in the list of available Altitude APs when configuring a WM-AD topology.

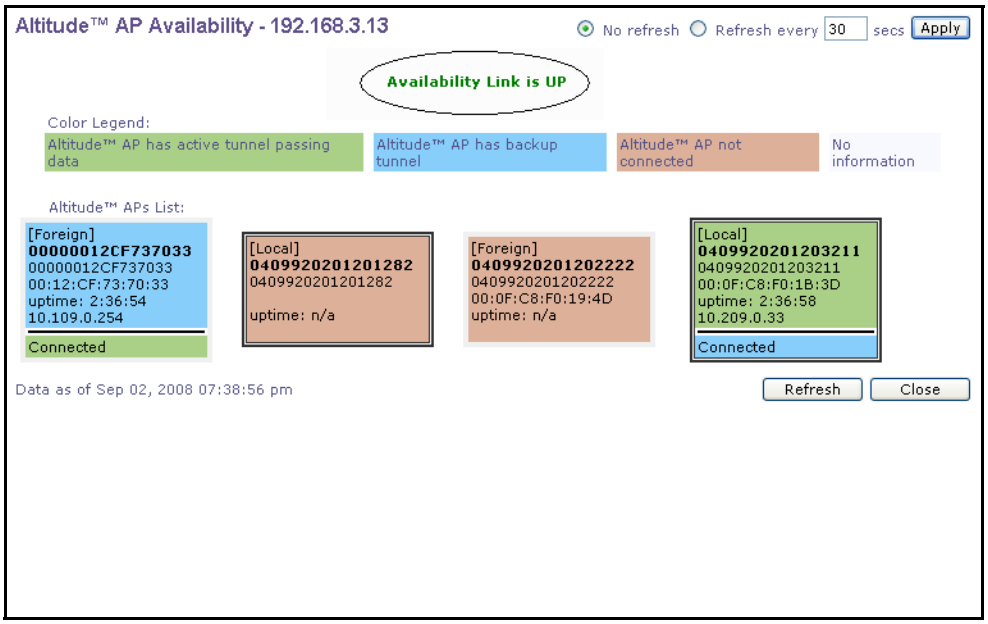
9 Verify that the 'availability' feature is configured correctly.

To verify the 'availability' feature is configured correctly:

a From the main menu of either of the two controllers, click **Reports and Displays**. The **Reports & Displays** page is displayed.


Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Port & WM-AD Filter Statistics
WM-AD Interface Statistics
Summit™ Controller Port Statistics
Altitude™ AP Availability
Dynamic Authorization Statistics
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
WDS WM-AD Altitude™ AP Statistics
Admission Control Statistics by Altitude™ AP
System Information
Client Location in Mobility Zone
Mobility Tunnel Matrix
Manufacturing Information
[WM| Summit WM2000 | 02 days, 02:43] User: admin Port status:
Software: V5 R3.10034.0

b From the **Reports & Displays** menu, click **Altitude AP Availability**. The **Altitude AP Availability Report** is displayed.



c Check the statement on the top of the page (as marked in the above screen shot).

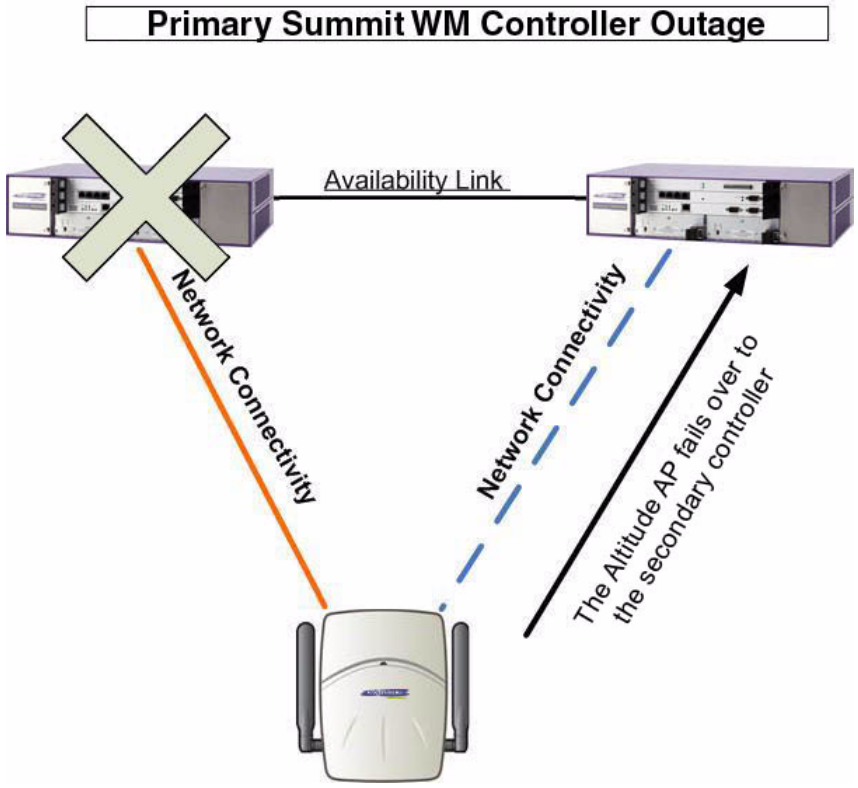
If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads Availability link is down, check the configuration error in logs. For more information on logs, see the *Summit WM Maintenance Guide*.

Session availability

The session availability feature enables the Altitude APs to switch over to a standby (secondary) Summit WM Controller fast enough to maintain the session availability (user session) in the following scenarios:

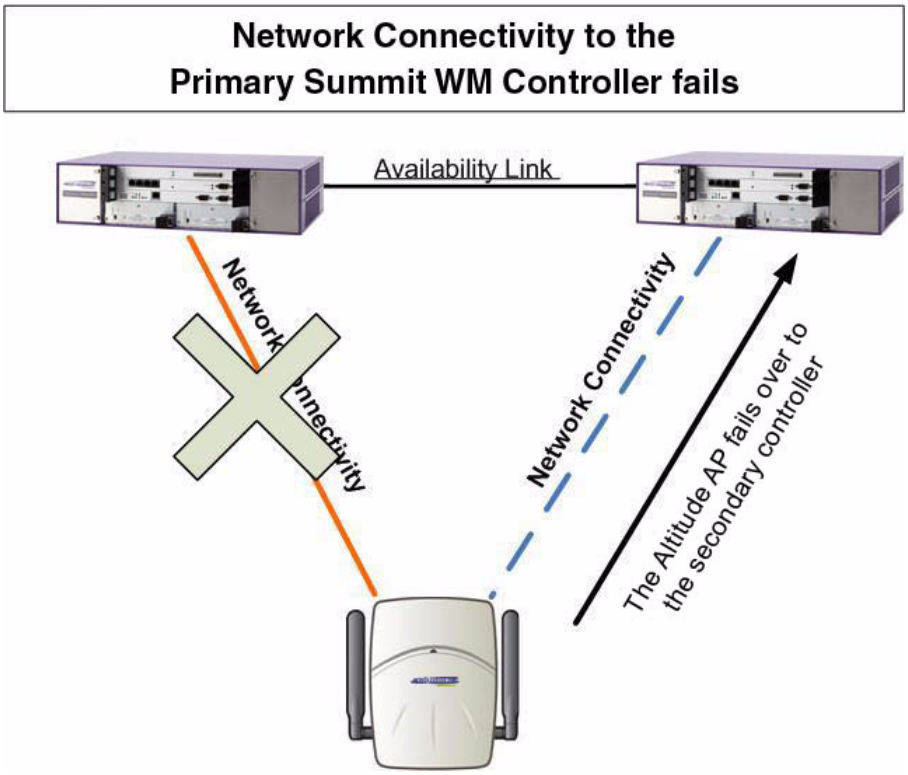
- The primary Summit WM Controller goes down

Figure 20: The Altitude AP fails over to the secondary controller when the primary controller goes down


Primary Summit WM Controller Outage
Availability Link
Network Connectivity
Network Connectivity
The Altitude AP fails over to the secondary controller

- The Altitude APs' network connectivity to the primary Summit WM Controller fails.

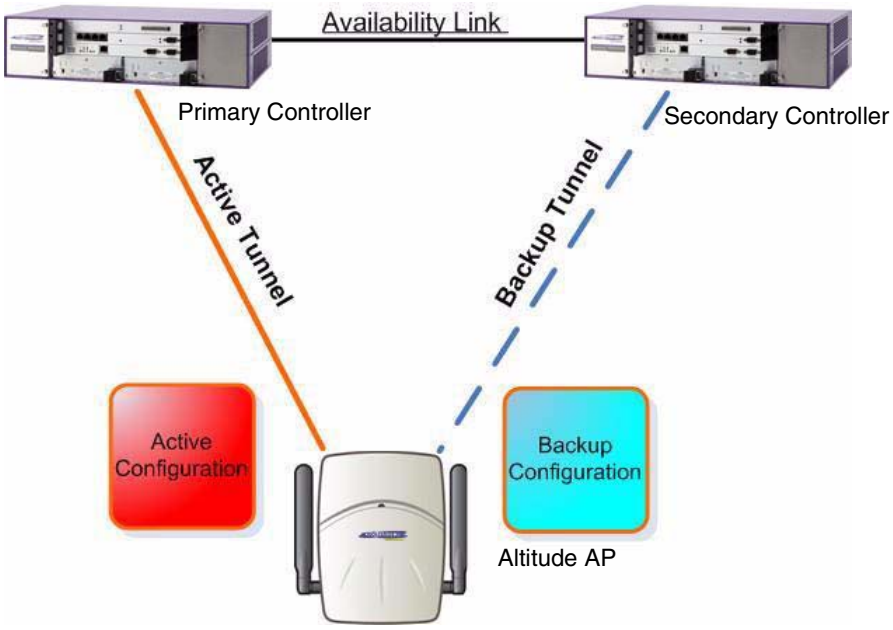
Figure 21: The Altitude AP fails over the secondary controller when the network connectivity to he primary controller fails



The secondary Summit WM Controller does not have to detect its link failure with the primary Summit WM Controller for the session availability to kick in. If the Altitude AP looses five consecutive polls to the primary controller either due to the controller outage or connectivity failure, it fails over to the secondary controller fast enough to maintain the user session.

In the session availability mode, the Altitude APs connect to both the primary and secondary Summit WM Controllers. While the connectivity to the primary Summit WM Controller is via the "active" tunnel, the connectivity to the secondary Summit WM Controller is via the "backup" tunnel.

Figure 22: Session availability mode



The following is the traffic flow of the topology illustrated in Figure 22:

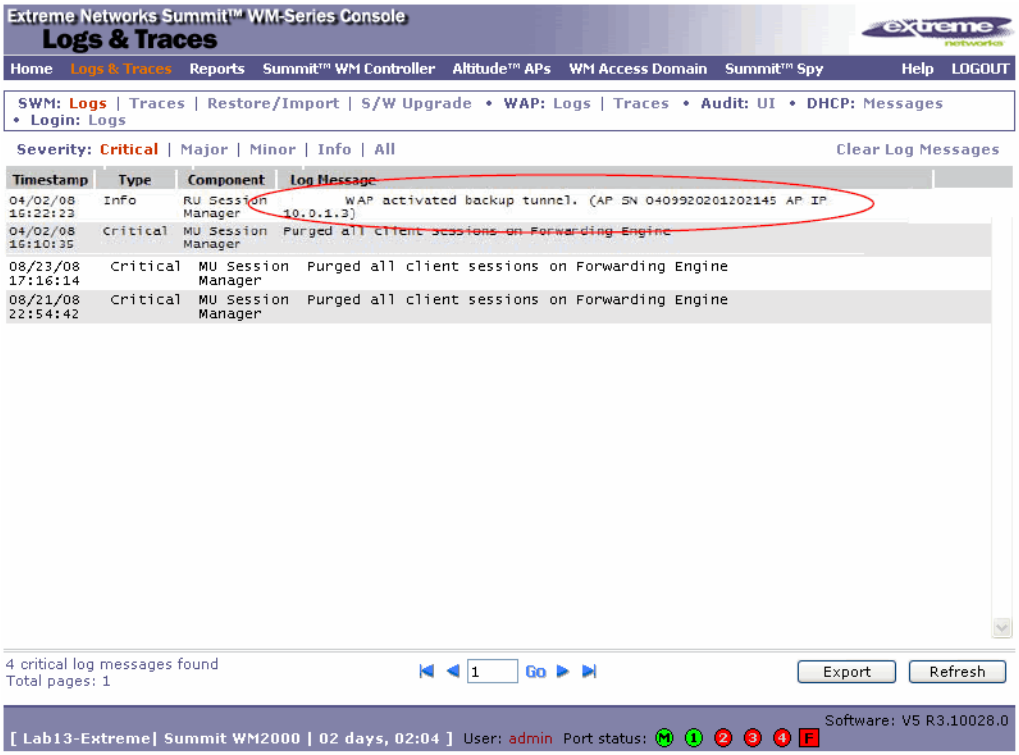
- The Altitude AP establishes active tunnel to connect to the primary Summit WM Controller.
- The Summit WM Controller sends the configuration to the Altitude AP. This configuration also contains the port information of the secondary Summit WM Controller.
- On the basis of the secondary Summit WM Controller's port information, the Altitude AP connects to the secondary controller via the backup tunnel.
- After the connection is established via the backup tunnel, the secondary Summit WM Controller sends the backup configuration to the Altitude AP.
- The Altitude AP receives the backup configuration and stores it in its memory to use it for failing over to the secondary controller. All this while, the Altitude AP is connected to the primary Summit WM Controller via the "active" tunnel.

Events and actions in session availability

In the event of the primary Summit WM Controller outage, or the network connectivity failure to the primary controller, the Altitude AP:

- Sends 'tunnel-active-req' request message to the secondary Summit WM Controller.
- The secondary Summit WM Controller accepts the request by sending the 'WASSP-tunnel-activate-response message.
- The Altitude AP applies the backup configuration and starts sending the data. The client devices' authentication state is not preserved during failover.

When the fast failover takes place, a critical message is displayed in the information log of the secondary Summit WM Controller.


Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
Severity: Critical | Major | Minor | Info | All
Clear Log Messages
Timestamp Type Component Log Message
04/02/08 16:22:23 Info RU Session Manager WAP activated backup tunnel. (AP SN 0409920201202145 AP IP 10.0.1.3)
04/02/08 16:10:35 Critical MU Session Manager Purged all client sessions on Forwarding Engine
08/23/08 17:16:14 Critical MU Session Manager Purged all client sessions on Forwarding Engine
08/21/08 22:54:42 Critical MU Session Manager Purged all client sessions on Forwarding Engine
4 critical log messages found
Total pages: 1
Go
Export
Refresh
Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 02 days, 02:04] User: admin Port status:

NOTE

In session availability, the maximum number of failover APs that the secondary controller can accommodate is equal to the maximum number of APs supported by the hardware platform and the license.

When the failed Summit WM Controller recovers, each Summit WM Controller in the pair goes back to normal mode. They exchange information that includes the latest lists of registered Altitude APs. The administrator must release the Altitude APs manually on the second Summit WM Controller, so that they may re-register with their home Summit WM Controller. Foreign APs can now all be released at once by using the **Foreign** button on the **Access Approval** page to select all foreign APs, and then clicking **Released**.

To support the availability feature during a failover event, administrators need to do the following:

1 Monitor the critical messages for the failover mode message, in the information log of the secondary Summit WM Controller (in the **Reports and Displays** section of the Summit WM Controller).

2 After recovery, on the secondary Summit WM Controller, select the foreign Altitude APs, and then click **Release** on the **Access Approval** page.

After the Altitude APs are released, they establish the active tunnel to their home controller and backup tunnel to the secondary controller.

Configuring session availability

Configuring session availability is a two-step process:

1 Configuring fast failover

2 Enabling session availability

NOTE

The 'fast failover' feature is a pre-requisite for session availability. To configure session availability, you must first configure the fast failover feature. For more information on how to configure fast failover, see "Configuring fast failover" on page 243.

In session availability, the user is able to retain the IP address. In addition, the user does not have to re-authenticate after the failover. These characteristics ensure that the failover is achieved within 5 seconds, which is fast enough to maintain the user's session.

NOTE

In session availability, the fast failover is achieved within 5 seconds only if there is at least one client device (mobile unit) associated to the Altitude AP. In the absence of any client device, the Altitude AP takes more time to failover since there is no need to preserve the user session.

NOTE

The session availability feature is a WM-AD attribute. It applies only to the following WM-ADs:

- Bridge Traffic Locally at WM
- Bridge Traffic Locally at AP

The users, who are on the conventional **Routed** WM-AD, are not benefitted by the session availability feature.

NOTE

Session availability is not support in a WM-AD that is configured for AAA network assignment.

Authentication state during failover

The authentication state is not preserved during fast failover. If a WM-AD requires authentication, the client device must re-authenticate. However, in such a case, the session availability is not guaranteed because authentication may require additional time during which the user session may be disrupted.

You must always use the following authentication mechanism for the fast failover configuration:

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access Privacy-Pre-Shared Key (WPA-PSK)

NOTE

Session availability is not supported in a WM-AD that uses Captive Portal (CP) authentication.

NOTE

Session availability does not support user-specific filters as these filters are not shared between the primary and secondary Summit WM Controllers.

Configuring fast failover

Before you configure the fast failover feature, you must ensure:

- The primary and secondary Summit WM Controllers are properly configured in 'availability' mode. For more information, see "Availability" on page 231.
- The pair of Summit WM Controllers in availability mode is formed by one of the following combinations:
  - WM200/2000 and WM200/2000
  - WM20 and WM20
  - WM200/2000 and WM20
- Both the primary and secondary Summit WM Controllers are running Summit WM Software V5R3 release.
- A network connection exists between the two Summit WM Controllers.
- The Altitude APs are operating in the 'availability' mode.
- The deployment is designed in such a way that the service provided by the Altitude APs is not dependent on which Summit WM Controller the APs associate with. For example, the fast failover feature will not support the deployment in which the two Summit WM Controllers in the availability mode are connected via a WAN link.
- Both the primary and secondary Summit WM Controllers have equivalent upstream access to the servers on which they depend. For example, both the controllers must have access to the same RADIUS and DHCP servers.
- The users (client devices) that use DHCP on WM-AD must obtain their addresses from a DHCP Server that is external to the Summit WM Controller.
- Time on all the network elements - both the Summit WM Controllers in availability pair, Altitude APs, DHCP and RADIUS servers etc.- is synchronized. For more information, see "Configuring network time" on page 56.

NOTE

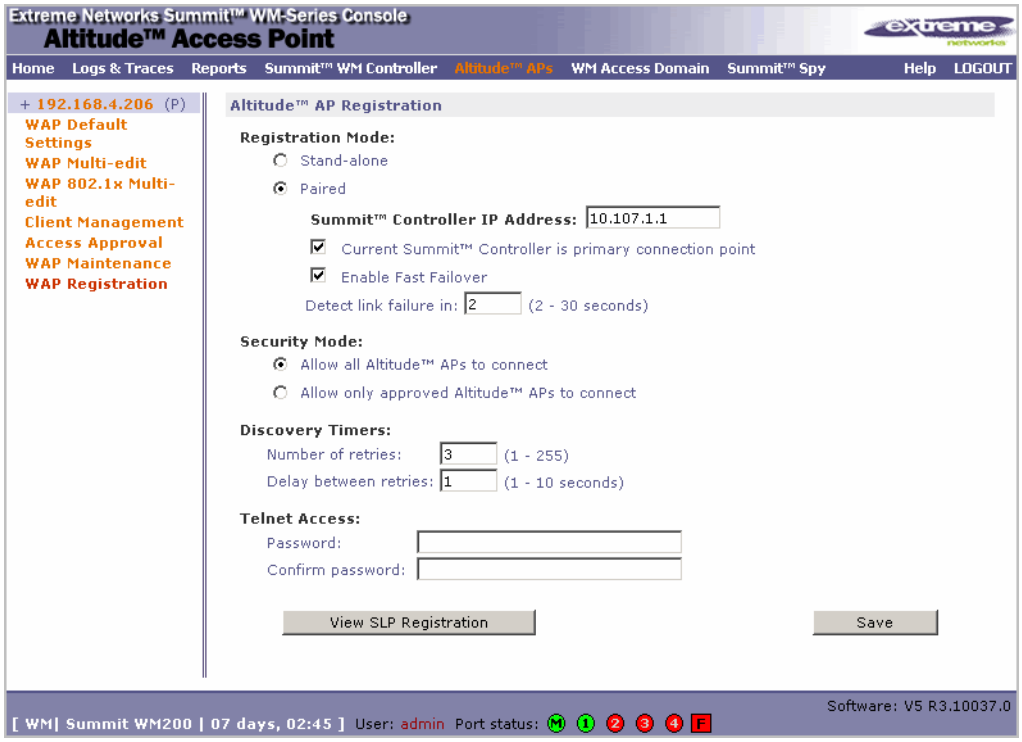
The fast failover feature works optimally in fast networks (preferably switched networks).

To configure the fast failover feature:

1 Log on both the primary and secondary Summit WM Controllers.

2 From the main menu of the primary Summit WM Controller, click **Altitude AP Configuration**. The **AP Properties** page is displayed.

3 In the left pane, click **WAP Registration**. The **WAP Registration** page is displayed.

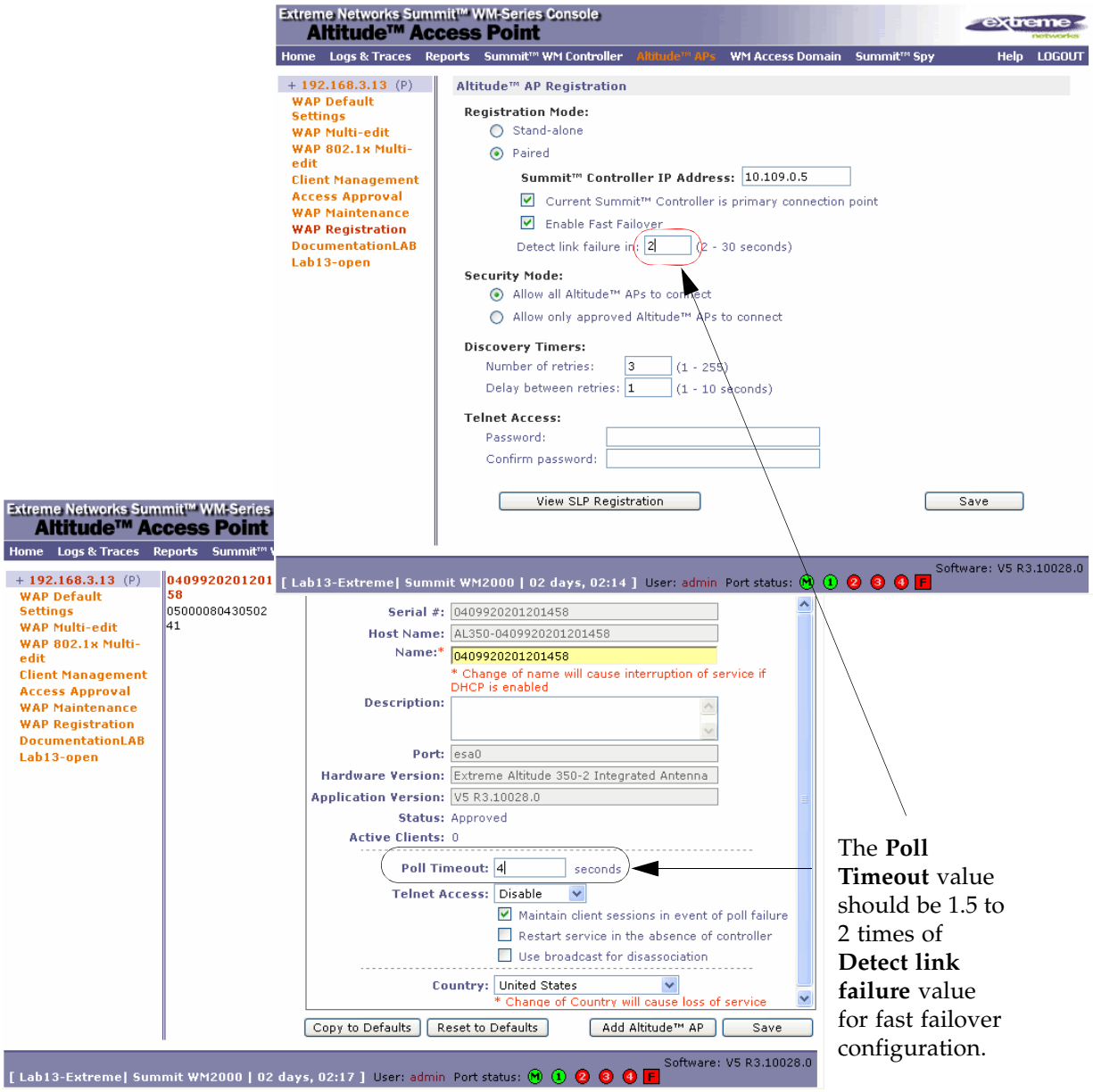


4 Select the **Enable Fast Failover** checkbox.

5 Type the appropriate value in **Detect link failure** box.

The **Detect link failure** field specifies the time period within which the system detects the link failure after the link has failed. For fast failover configuration, this parameter is tied closely to the **Poll Timeout** parameter on the **WAP Registration** page. The **Poll Timeout** field specifies the time period for which the Altitude AP waits before re-attempting to establish a link when its polling to the primary Summit WM Controller fails.

For the fast failover feature to work within the time frame of 5 seconds, the **Poll Timeout** value should be 1.5 to 2 times o**f Detect link failure** value. For example, if you have set the **Detect link failure** value to 2 seconds, the **Poll Timeout** value should be set to 3 or 4 seconds.



The **Poll Timeout** value should be 1.5 to 2 times of **Detect link failure** value for fast failover configuration.

6 Set the Altitude APs **Poll Timeout** value for fast failover.

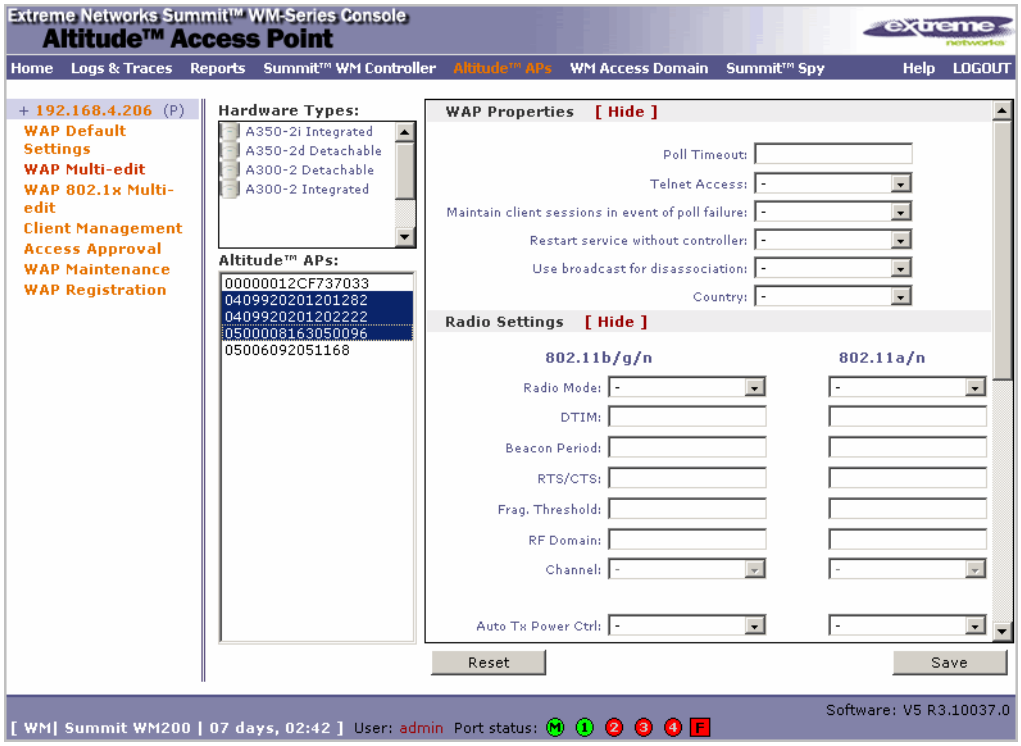
To set the Poll Timeout value for fast failover:

a From the main menu of the primary Summit WM Controller, click **Altitude AP Configuration**. The **AP Properties** page is displayed.

b In the left pane, click **AP Multi-edit**. The **AP Multi-edit** page is displayed.

c In the **Hardware Types** list, select the hardware type of the Altitude APs that are part of your deployment. You can select multiple hardware types by pressing the **CTRL** key and clicking the hardware in the **Hardware Types** list.

d In the **Altitude APs** list, select the Altitude APs for which you want to set the **Poll Timeout** value. You can select multiple Altitude APs by pressing the **CTRL** key and clicking the **Altitude APs** in the Altitude APs list.



e In the **Poll Timeout** box, type/edit the appropriate value.

f To save your changes, click **Save**.

7 From the main menu of the secondary Summit WM Controller, click **Altitude AP Configuration**. The **AP Properties** page is displayed.

8 Select the **Enable fast failover** checkbox.

9 Set the **Detect link failure** value and the **Poll Timeout** value as explained in Step 5.

NOTE

The fast failover configuration must be identical on both the primary and secondary Summit WM Controllers. Logs are generated if the configuration is not identical. For more information, see the Summit WM Controller, Access Points and Convergence Software Maintenance Guide.

After you have configured fast failover, you must configure session availability to preserve the user session during the failover.

Enabling session availability

Before you enable session availability, you must ensure:

- The primary and secondary Summit WM Controllers are properly configured in 'availability' mode. For more information, see "Availability" on page 231.
- The fast failover feature is properly configured. For more information, see "Configuring fast failover" on page 243.

NOTE

If you haven't configured the fast failover feature, the Enable Session Availability checkbox is not displayed on the WM-ADs page.

- Time on all the network elements - both the Summit WM Controllers in availability pair, Altitude APs, DHCP and RADIUS servers etc.- is synchronized. For more information, see "Configuring network time" on page 56.
- Both the Summit WM Controllers in fast failover mode must be running Summit WM Software V5R3 release.

NOTE

Session availability applies only to the following WM-ADs:
- Bridge Traffic Locally at WM
- Bridge Traffic Locally at AP

NOTE

*If you are using **Bridge Traffic Locally at WM WM-AD**, you must select **None** from the **DHCP Option** drop-down menu on the Topology page.*

NOTE

*The **Bridge Traffic Locally at WM** must be mapped to the same VLAN on both the primary and secondary Summit WM Controllers.*

To enable session availability:

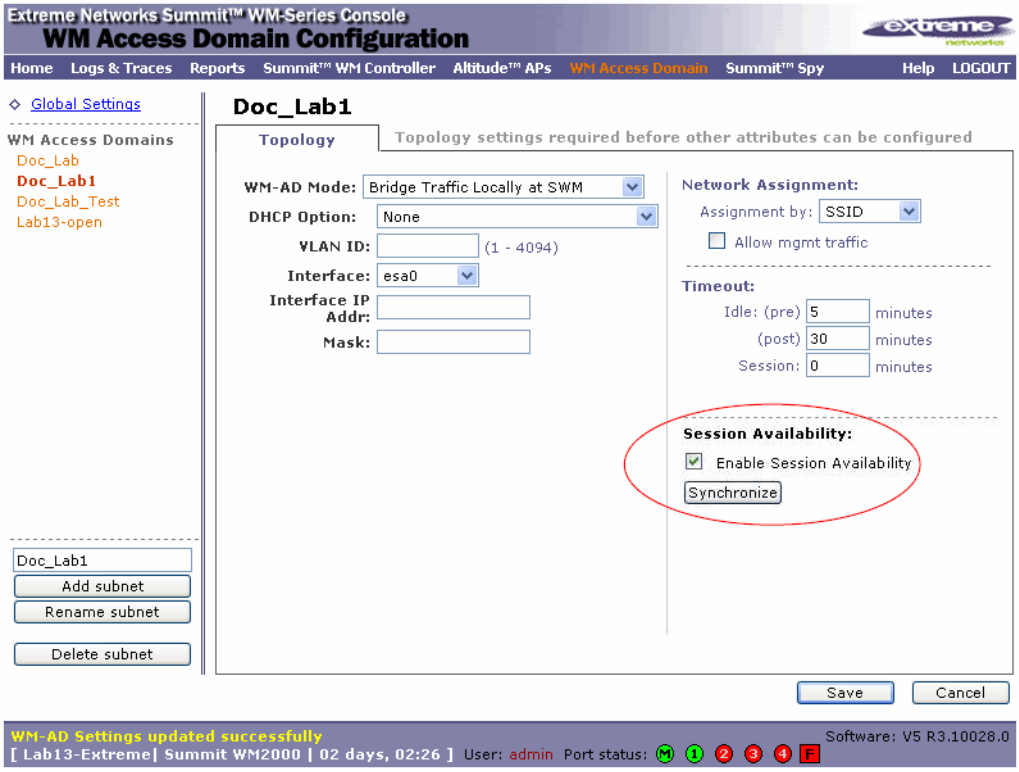
1 Log on both the primary Summit WM Controller and secondary Summit WM Controller.

2 From the main menu of the primary Summit WM Controller, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

3 In the left pane, select the WM-AD for which you want to enable the session availability during the fast failover.

4 Select the **Enable Session Availability** checkbox.

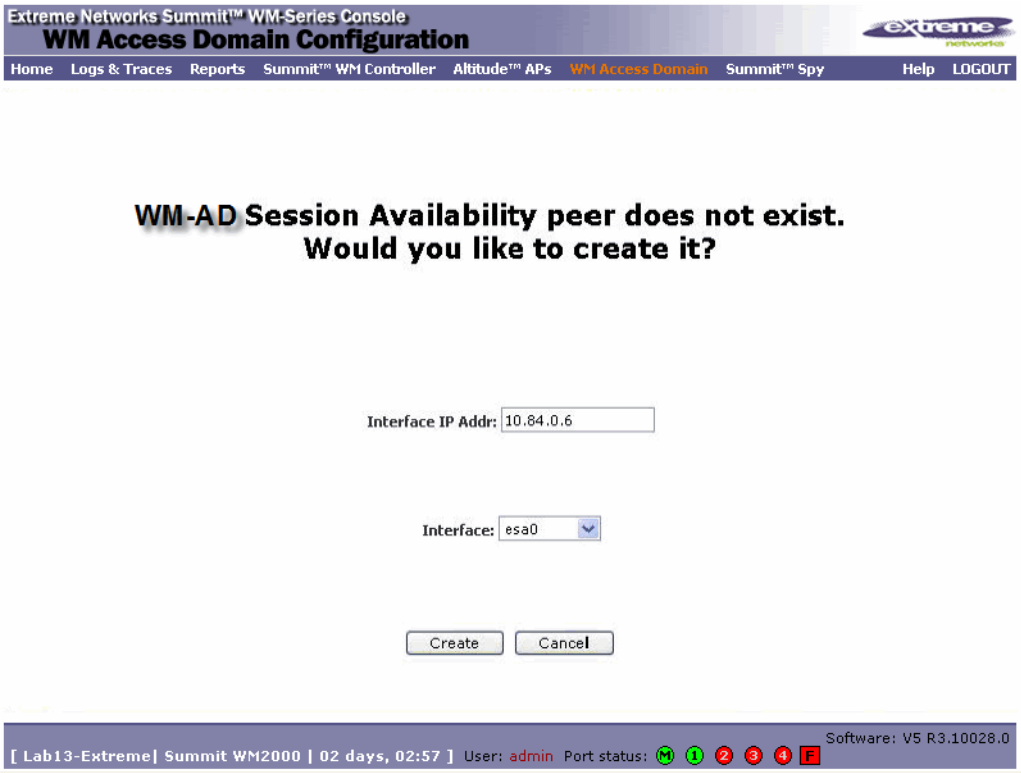
When you select the **Enable Session Availability** checkbox for a specific WM-AD, the user-sessions are prioritized during the failover on this WM-AD. The sessions are registered on "first come-first serve" basis.



NOTE

*If you are using **Bridge Traffic Locally at WM WM-AD**, the WM-AD must have the **DHCP Option** configured as **None**.*

5 If the same WM-AD (WM-AD peer) is not configured on the secondary Summit WM Controller, click **Synchronize**. The following page is displayed.


Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
WM-AD Session Availability peer does not exist.
Would you like to create it?
Interface IP Addr: 10.84.0.6
Interface: esa0
Create Cancel
[Lab13-Extreme| Summit WM2000 | 02 days, 02:57] User: admin Port status: M 1 2 3 4 F
Software: V5 R3.10028.0

6 In the **Interface IP addr** box, type the secondary Summit WM Controller's interface IP address.

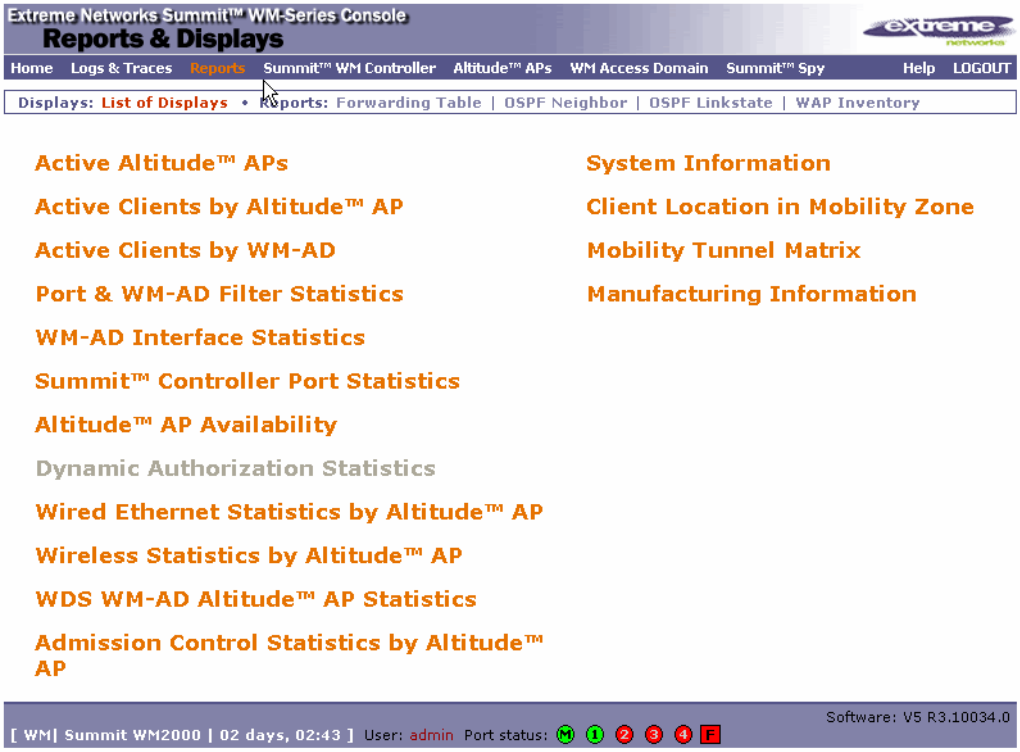
7 From the **Interface** drop-down menu, select the secondary Summit WM Controller's physical port.

8 Click **Create**. The system creates a WM-AD peer on the secondary Summit WM Controller by copying the WM-AD parameters.

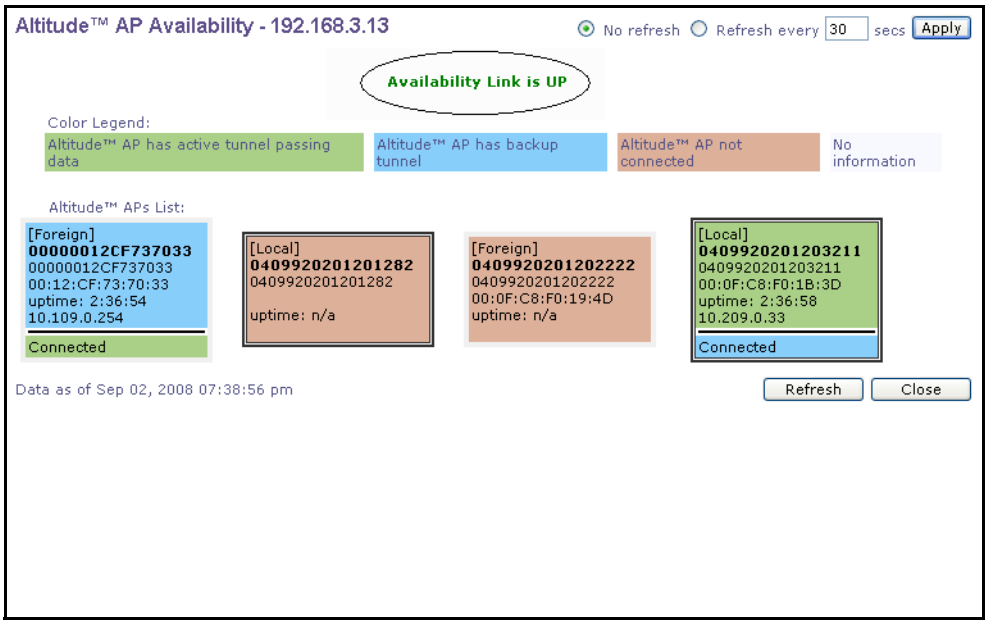
9 Verify that the session availability feature is configured correctly.

To verify the session availability feature is configured correctly:

a From the main menu of either of the two controllers, click **Reports and Displays**. The **Reports & Displays** page is displayed.


Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Port & WM-AD Filter Statistics
WM-AD Interface Statistics
Summit™ Controller Port Statistics
Altitude™ AP Availability
Dynamic Authorization Statistics
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
WDS WM-AD Altitude™ AP Statistics
Admission Control Statistics by Altitude™ AP
System Information
Client Location in Mobility Zone
Mobility Tunnel Matrix
Manufacturing Information
Software: V5 R3.10034.0
[WM] Summit WM2000 | 02 days, 02:43] User: admin Port status: M 1 2 3 4 F

b From the **Reports and Displays** menu, click **Altitude AP Availability**. The **Altitude AP Availability Report** is displayed.



c Check the statement at the top of the page (as marked in the above screen shot).

10 If the statement reads **Availability link is up**, the availability feature is configured correctly. If the statement reads **Availability link is down**, check the configuration error in logs. For more

information on logs, see the Summit WM Controller, Access Points and Convergence Software Maintenance Guide.

Viewing the Altitude AP availability display

Viewing SLP activity

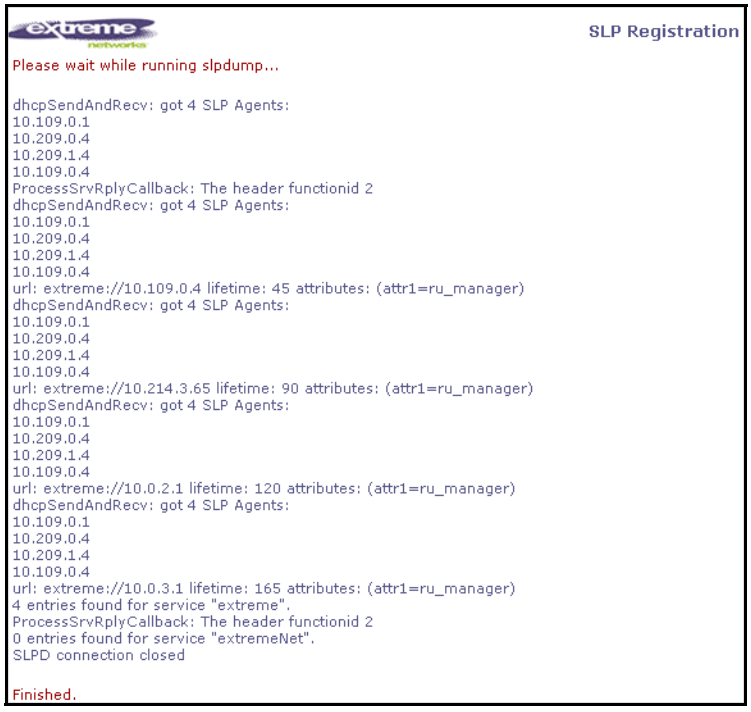
In normal operations, the primary Summit WM Controller registers as an SLP service called ac_manager. The controller service directs the Altitude APs to the appropriate Summit WM Controller. During an outage, if the remaining Summit WM Controller is the secondary controller, It registers as the SLP service ru_manager.

To view SLP activity:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude APs registration** page is displayed.

2 In the left pane, click **AP Registration**. The **Altitude AP Registration** page is displayed.

3 To confirm SLP registration, click V**iew SLP Registration**. A pop-up page displays the results of the diagnostic slpdump tool, to confirm SLP registration.



7 Mobility

This chapter describes the mobility concept, including:

- "Mobility overview" on page 253
- "Mobility domain topologies" on page 254
- "Configuring mobility domain" on page 256

Mobility overview

The Summit WM Software system allows multiple Summit WM Controllers (up to 12) on a network to discover each other and exchange information about a client session. This technique enables a wireless device user to roam seamlessly between different Altitude APs on different Summit WM Controllers.

The solution introduces the concept of a mobility manager; one Summit WM Controller on the network is designated as the mobility manager and all others are designated as mobility agents.

The wireless device keeps the IP address, WM-AD assignment, and filtering rules it received from its home Summit WM Controller - the Summit WM Controller that it first connected to. The WM-AD on each Summit WM Controller must have the same SSID and RF privacy parameter settings.

For the mobility manager you have two options:

- Rely on SLP with DHCP Option 78
- Define at the agent the IP address of the mobility manager. By explicitly defining the IP address, the agent and the mobility manager are able to find each other directly without using the SLP discovery mechanisms. Direct IP definition is recommended in order to provide tighter control of the registration steps for multi-domain installations.

The Summit WM Controller designated as the mobility manager:

- The mobility manager is explicitly identified as the manager for a specific mobility domain. Agents will connect to this manager to establish a mobility domain.
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Uses SLP, if this method is preferred, to register itself with the SLP Directory Agent as ExtremeNet.
- Defines the registration behavior for a multi-controller mobility domain set:
  - **Open mode** - A new agent is automatically able to register itself with the mobility manager and immediately becomes part of the mobility domain
  - **Secure mode** - The mobility manager does not allow a new agent to automatically register. Instead, the connection with the new agent is placed in pending state until the administrator approves the new device.
- Listens for connection attempts from mobility agents.
- Establishes connection and sends a message to the mobility agent specifying the Heartbeat interval, and the mobility manager's IP address if it receives a connection attempt from the agent.

- Sends regular Heartbeat messages containing wireless device session changes and agent changes to the mobility agents and waits for a returned update message

The Summit WM Controller designated as a mobility agent:

- Uses SLP or a statically configured IP address to locate the mobility manager
- Defines at the agent the IP address of the mobility manager, which allows for the bypass of SLP. Agents directly find and attempt to register with the mobility manager.
- Attempts to establish a TCP/IP connection with the mobility manager
- In response to the 'heartbeat' message, the mobility agent sends updates on the wireless device users and the data tunnels to the mobility manager.

If a controller configured as the mobility manager is lost, the following occurs:

- Agent to agent connections will remain active.
- Mobility agents will continue to operate based on the mobility information last coordinated before the manager link was lost. The mobility location list remains relatively unaffected by the controller failure. Only entries associated with the failed controller are cleared from the registration list, and users that have roamed from the manager controller to other agents are terminated and required to re-register as local users with the agent where they are currently located.
- Participant controllers are reset to nodal operation
- Any user sessions that roamed away from their home AP are terminated and must reconnect
- Users need to reconnect to network, re-authenticate, and obtain new IP address
- The data link between active controllers remains active after the loss of a mobility manager
- Mobility agents continue to use the last set of mobility location list to service known users
- Existing users:
  - Existing users remain in mobility scenario, and if the users are known to mobility domain, they continue to be able to roam between connected controllers
- New users:
  - New users become local at attaching controller
  - Roaming to another controller resets session

NOTE

The mobility network that includes all the Summit WM Controllers and the Altitude APs is called Mobility Domain.

NOTE

The mobility feature is not backward compatible. This means that all the Summit WM Controllers in the mobility domain must be running Summit WM Software V5R3 release.

Mobility domain topologies

You can configure the mobility domain with the following topologies:

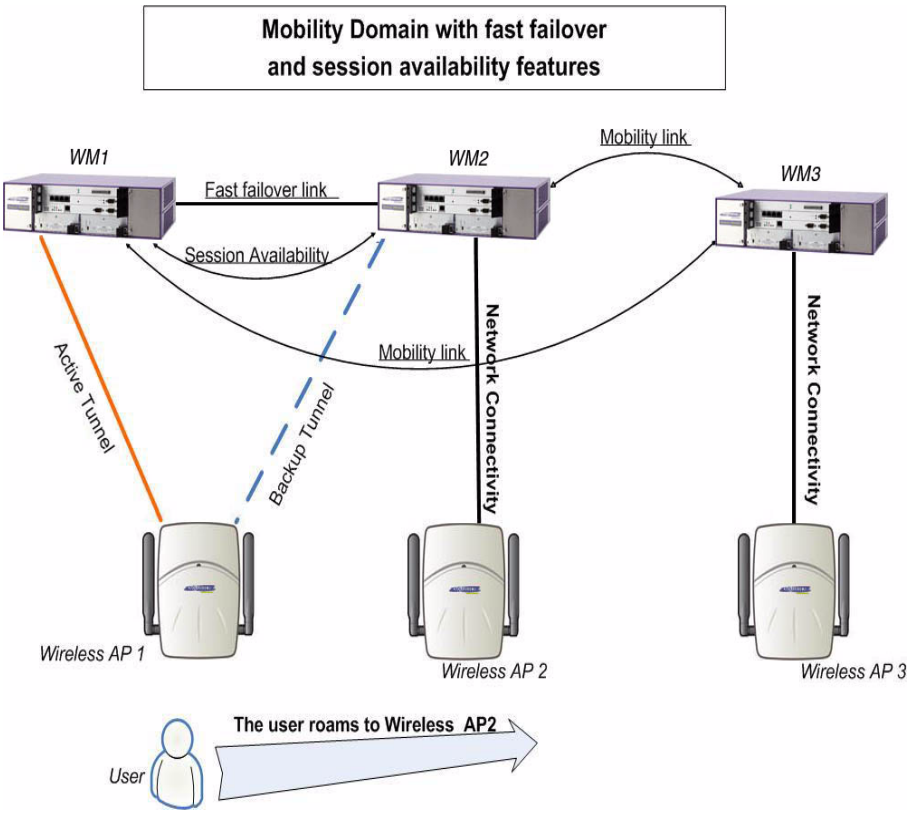
- Mobility domain without any availability
- Mobility domain with availability

- Mobility domain with session availability

NOTE

If you are configuring mobility, you must synchronize time on all the Summit WM Controllers that are part of the mobility domain. For more information, see "Configuring network time" on page 56.

Figure 23: Mobility Domain with fast failover and session availability features



- WM1 and WM2 are configured for session availability.
- WM1, WM2, WM3, Wireless AP1, Wireless AP2 and Wireless AP3 form a Mobility Domain
- WM3 is the Mobility Manager whereas WM1 and WM2 are Mobility Agents

- The user's home session is with WM1.
- When the user roams from Wireless AP 1 to Wireless AP 2, he establishes his home session with WM2.
- When the user roams, the Wireless AP 1 receives a notification that the user has roamed away following which it marks the user session as "inactive". Consequently, no statistics are sent to the WM1 for that user.
- In response to the heart beat message from the mobility manager (WM3), the WM2 sends updates that the user has a new home on WM2. Upon receiving the updates, the mobility manager updates its own tables.

NOTE

The mobility manager's heart beat time is configurable. If you are configuring mobility domain with session availability, you should configure the heart beat time as one second in order to enable the mobility manager to update its tables fast.

- If the failover takes place, and the user is still associated with Wireless AP1:
  - The Wireless AP 1 fails over, and establishes active session with WM2.
  - In response to the heart beat message from the mobility manager (WM3), the WM2 sends updates to the mobility manager on the failover Wireless AP and its user.
- If the failover takes place, and the user has roamed to Wireless AP 2:
  - As part of roaming, the user's home session moves from WM1 to WM2.
  - Wireless AP 1 establishes active session with WM 2. Wireless AP 2 is not impacted by the failover.

NOTE

The mobility feature is not backward compatible. This means that all the Summit WM Controllers in the mobility domain must be running Summit WM Software V5R3 release.

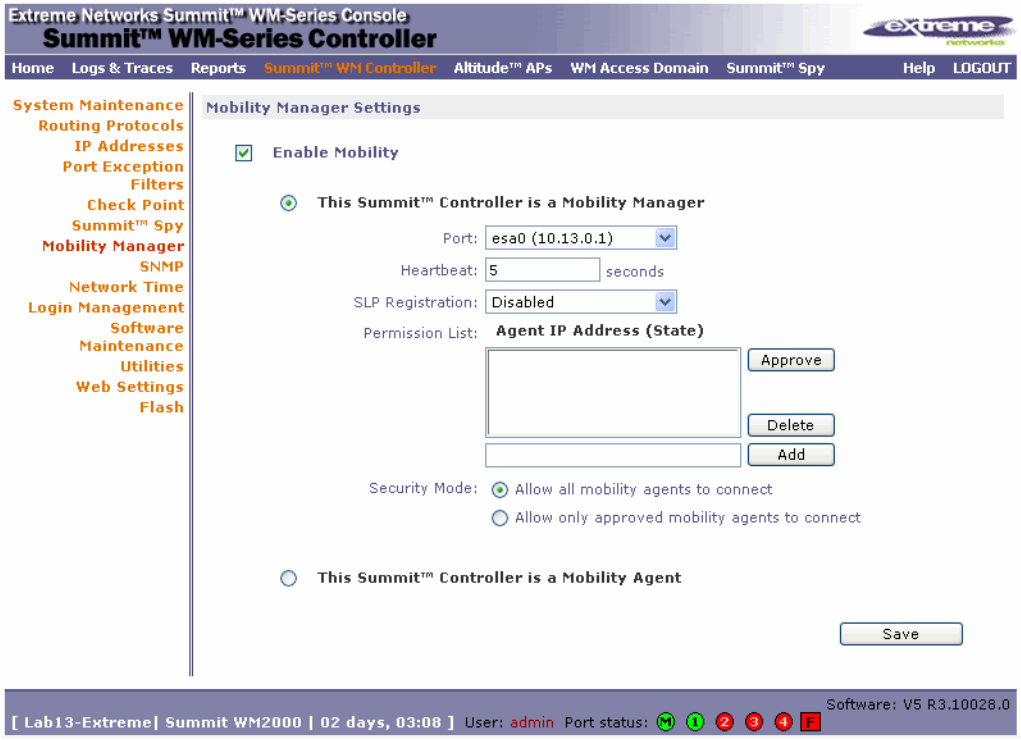
Configuring mobility domain

If you are configuring the mobility domain with availability or session availability, you must synchronize time on all the Summit WM Controllers that are part of your mobility domain. For more information, see "Configuring network time" on page 56.

To designate a mobility manager:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** page is displayed.

2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** page is displayed.



3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options appear.

4 Select the **This Summit Controller is a Mobility Manager** option. The mobility manager options appear.

5 In the **Port** drop-down list, click the interface on the Summit WM Controller to be used for the mobility manager process. Ensure that the selected interface is routable on the network.

6 In the **Heartbeat** box, type the time interval (in seconds) at which the mobility manager sends a Heartbeat message to a mobility agent.

NOTE

If the mobility domain is configured for fast failover and session availability, you should configure the mobility manager's heart beat time as one second.

7 In the **SLP Registration** drop-down list, click whether to enable or disable SLP registration.

8 In the **Permission** list, click the agent IP addresses you want to approve that are in pending state, by selecting the agent and clicking **Approve**. New agents are only added to the domain if they are approved.

You can also add or delete controllers that you want to be part of the mobility domain. To add a controller, type the agent IP address in the box, and then click **Add**. To delete a controller, click the controller in the list, and then click **Delete**.

9 Select the Security Mode option:

- **Allow all mobility agents to connect** - All mobility agents can connect to the mobility manager.
- **Allow only approved mobility agents to connect** - Only approved mobility agents can connect to the mobility manager.

10 To save your changes, click **Save**.

NOTE

If you set up one Summit WM Controller on the network as a mobility manager, all other Summit WM Controllers must be set up as mobility agents.

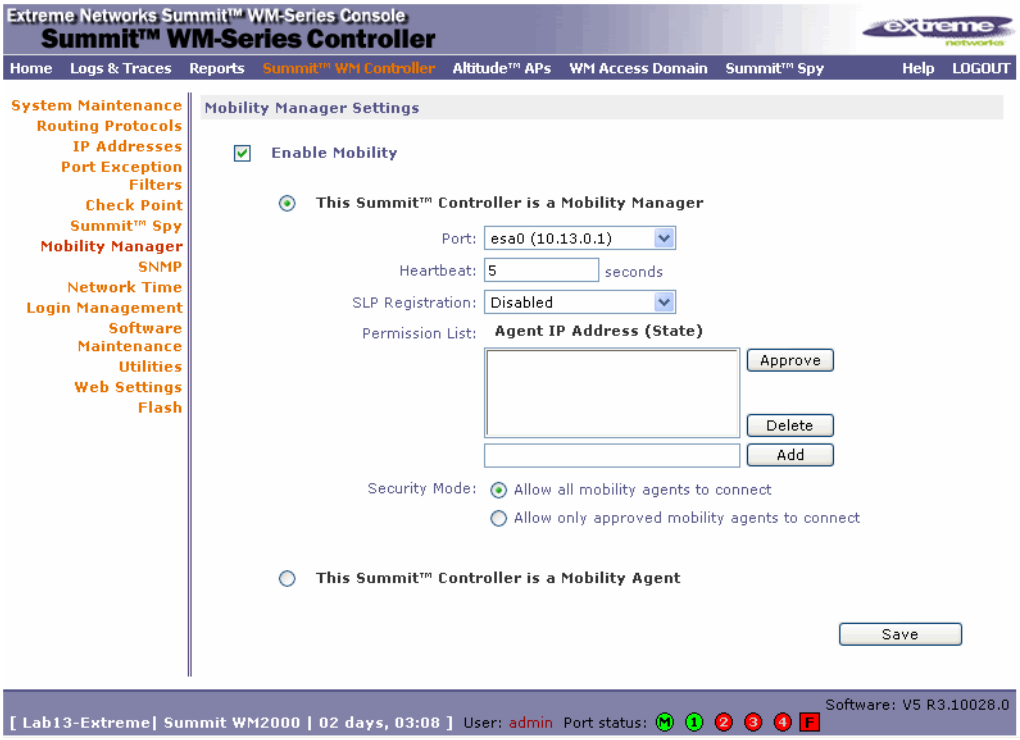
To designate a mobility agent:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** page is displayed.

2 In the left pane, click **Mobility Manager**. The **Mobility Manager Settings** page is displayed.

3 To enable mobility for this controller, select the **Enable Mobility** checkbox. The controller mobility options are displayed,

4 Select the **This Summit Controller is a Mobility Agent** option. The mobility agent options are displayed.



5 From the **Port** drop-down list, click the port on the Summit WM Controller to be used for the mobility agent process. Ensure that the port selected is routable on the network.

6 In the **Heartbeat** box, type the time interval (in seconds) to wait for a connection establishment response before trying again.

NOTE

The mobility agent's heartbeat value should be similar to mobility manager's heartbeat value.

7 From the **Discovery Method** drop-down list, click one of the following:

- **SLPD** - Service Location Protocol Daemon is a background process acting as a SLP server. It provides the functionality of the Directory Agent and Service Agent for SLP. Use SLP to support the discovery of Extreme service to attempt to locate the area mobility manager controller.
- **Static Configuration** - Select Static Configuration if you want to enter the IP address of the mobility manager manually. Defining a static configuration for a mobility manager IP address bypasses SLP discovery.

8 In the **Mobility Manager Address** box, type the IP address for the designated mobility manager.

9 To save your changes, click **Save**.

Displays for the mobility manager

For more information, see "Viewing displays for the mobility manager" on page 283.

8 Working with third-party APs

You can set up the Summit WM Controller to handle wireless device traffic from third-party access points, providing the same policy and network access control. This process requires the following steps:

- Step 1 - Define a data port as a third party AP port
- Step 2 - Define a WM-AD for the third-party AP port
- Step 3 - Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD
- Step 4 - Define filtering rules for the third-party APs

CAUTION

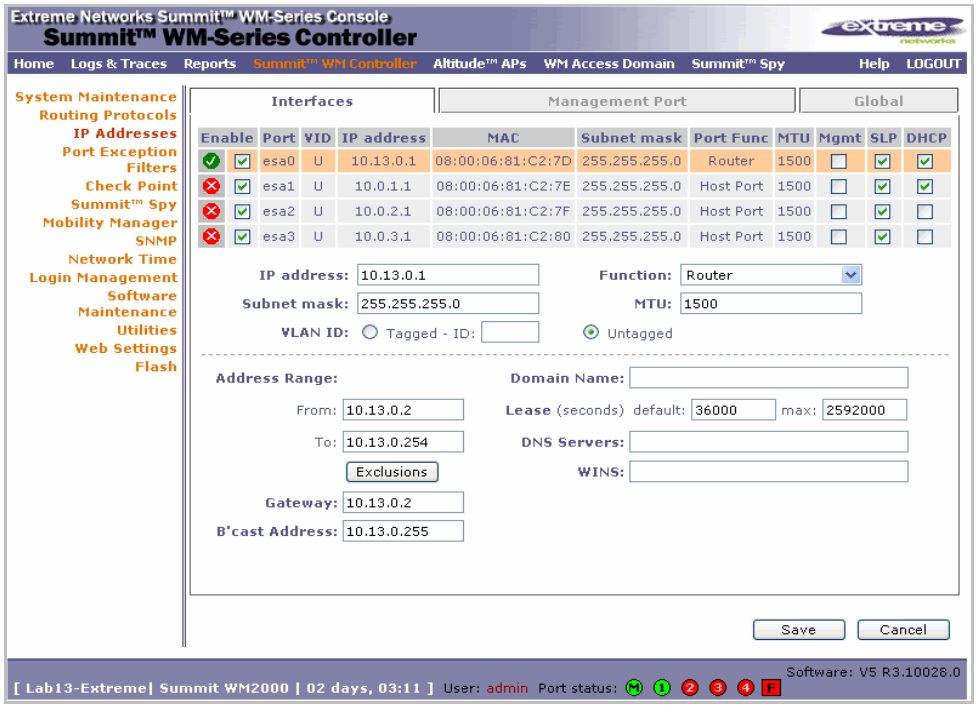
The Outdoor AP is not a third party AP. The Outdoor AP is fully managed by the Summit WM controller just like an Altitude AP.

Setting up third-party APs

Step 1 - Define a data port as a third party AP port

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 From the left pane, click **IP Address**. The **Management Port Settings and Interfaces** page is displayed.



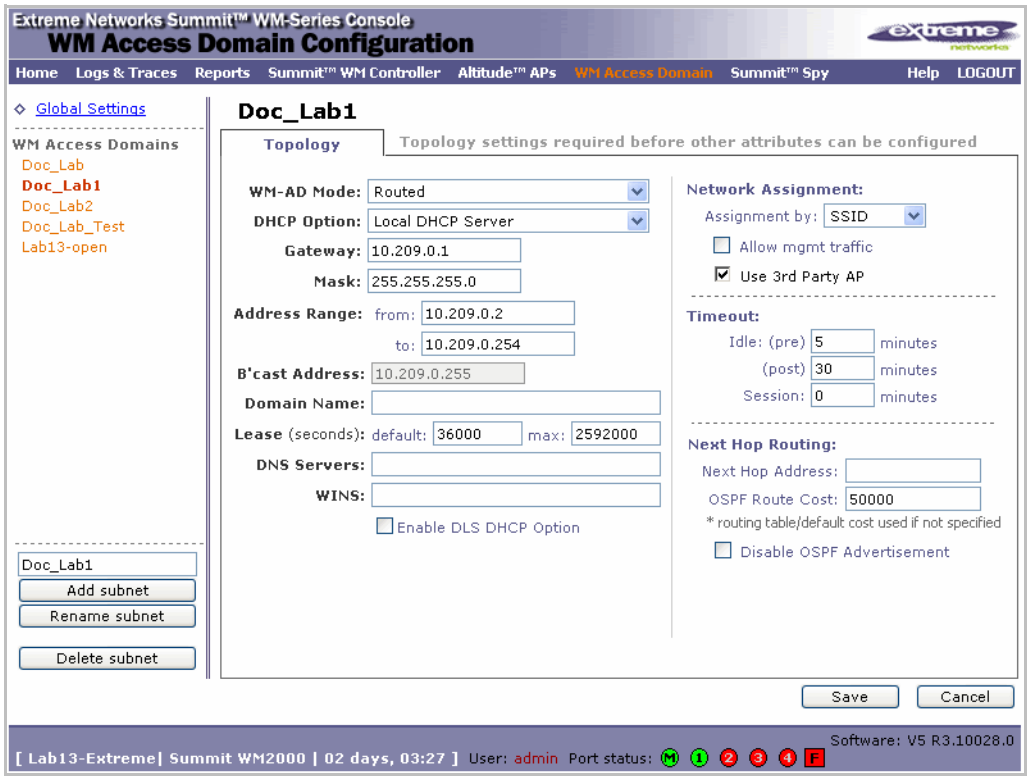
3 Click the port, and in the **Function** box, click **3rd-party AP** from the drop-down list. Make sure that Management Traffic and SLP are disabled for this port.

4 Connect the third-party access point to this port, via a switch.

Step 2 - Define a WM-AD for the third-party AP port

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** page is displayed.

2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box, and then click **Add subnet**. The name is displayed in the **WM Access Domains** list. The **Topology** tab is displayed.



3 In the **Assignment by** drop-down list, click **SSID**.

4 To define a WM-AD for a third-party AP, select the **Use 3rd Party AP** checkbox.

5 Continue configuring your WM-AD, as described in "Configuring topology for a WM-AD for Captive Portal" on page 157.

NOTE

Bridge Traffic at AP and MAC-based authentication are not available for third-party WM-ADs.

Step 3 - Define authentication by Captive Portal and RAD policy for the third-party AP WM-AD

1 Click the **Auth & Acct** tab.

2 In the **Authentication Configuration** page, click **Configure Captive Portal Settings**.

3 In the **Captive Portal Settings** page, define the Captive Portal configuration.

4 Click the **RAD Policy** tab.

5 Define the filter IDs to match those in RADIUS server.

Step 4 - Define filtering rules for the third-party APs

1 Because the third-party APs are mapped to a physical port, you must define the Exception filters on the physical port, using the **Port Exception Filters** page. For more information, see "Configuring filtering rules for a WM-AD" on page 181.

2 Define filtering rules that allow access to other services and protocols on the network such as HTTP, FTP, Telnet, SNMP.

In addition, modify the following functions on the third-party access point:

- Disable the access point's DHCP server, so that the IP address assignment for any wireless device on the AP is from the DHCP server at the Summit WM Controller with WM-AD information.
- Disable the third-party access point's layer-3 IP routing capability and set the access point to work as a layer-2 bridge.

Here are the differences between third-party access points and Wireless APs on the Summit WM Controller, Access Points, and WM software system:

- A third-party access point exchanges data with the Summit WM Controller's data port using standard IP over Ethernet protocol. The third-party access points do not support the tunnelling protocol for encapsulation.
- For third-party access points, the WM-AD is mapped to the physical data port and this is the default gateway for mobile units supported by the third-party access points.
- A Summit WM Controller cannot directly control or manage the configuration of a third-party access point.
- Third-party access points are required to broadcast an SSID unique to their segment. This SSID cannot be used by any other WM-AD.
- Roaming from third-party access points to Wireless APs and vice versa is not supported.

9 Working with the Summit WM series Spy

This chapter describes Summit WM series Spy concepts, including:

- "Summit WM series Spy overview" on page 263
- "Enabling the Analysis and data collector engines" on page 264
- "Running Summit WM series Spy scans" on page 265
- "Analysis engine overview" on page 267
- "Working with Summit WM series Spy scan results" on page 268
- "Working with friendly APs" on page 270
- "Maintaining the Summit WM series Spy list of APs" on page 271
- "Viewing the Scanner Status report" on page 272

Summit WM series Spy overview

The Summit WM series Spy is a mechanism that assists in the detection of rogue APs. Summit WM series Spy functionality does the following:

Altitude AP:

- Runs a radio frequency (RF) scanning task.
- Alternating between scan functions, providing its regular service to the wireless devices on the network.

NOTE

If a Wireless AP is part of a WDS link you cannot configure it to act as a scanner in Summit WM series Spy.

Summit WM Controller:

- Runs a data collector application that receives and manages the RF scan messages sent by the Wireless AP. RF data collector data includes lists of all connected Wireless APs, third-party APs, and the RF scan information that has been collected from the Wireless APs selected to perform the scan.
- Runs an Analysis Engine that processes the scan data from the data collector through algorithms that make decisions about whether any of the detected APs or clients are rogue APs or are running in an unsecure environment (for example, ad-hoc mode).

NOTE

In a network with more than one Summit WM Controller, it is not necessary for the data collector to be running on the same controller as the Analysis Engine. One controller can be a dedicated Analysis Engine while the other controllers run data collector functionality. No more than one Analysis Engine can be running at a time. You must ensure that the controllers are all routable.

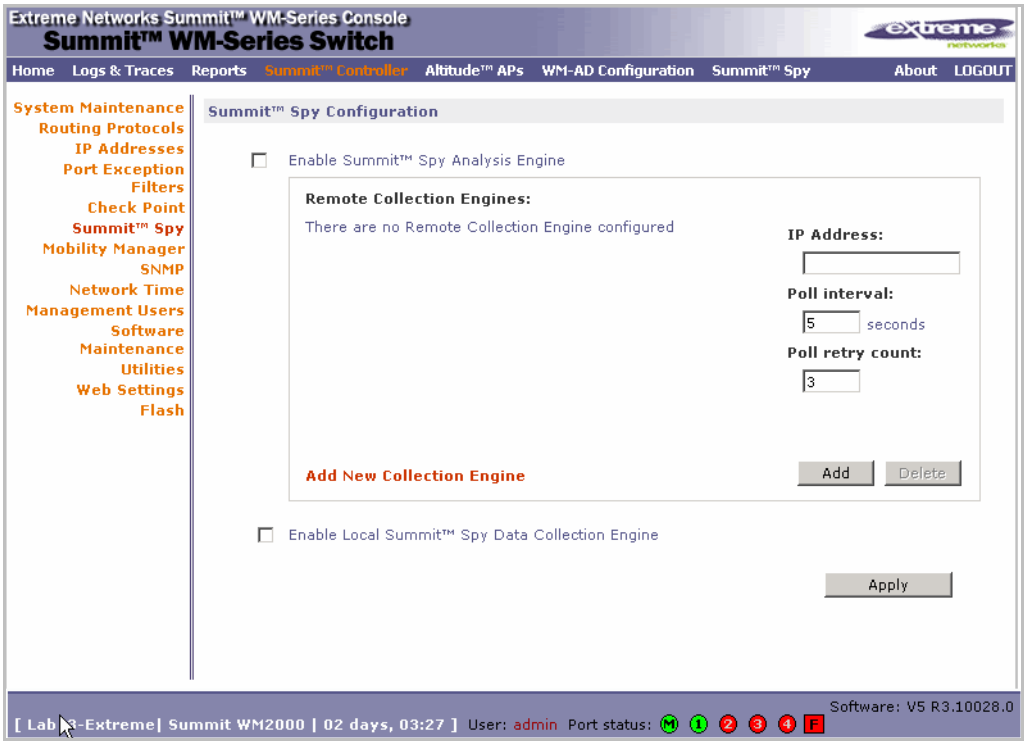
Enabling the Analysis and data collector engines

Before using the Summit WM series Spy, you must enable and define the Analysis and data collector engines.

To enable the Analysis engine:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Summit Spy**. The **Summit Spy Configuration** page is displayed.



3 To enable the Summit WM series Spy Analysis Engine, select the **Enable Summit Spy Analysis Engine** checkbox.

4 To enable the Summit Spy Data Collection Engine on this Summit WM Controller, select the **Enable Local Summit Spy Data Collection Engine** checkbox.

5 To identify the remote RF Data Collector Engine that the Analysis Engine will poll for data, type the IP address of the Summit WM Controller on which the remote Data Collector resides in the **IP Address** box.

NOTE

Currently, the Summit WM Controller WM20 does not support the Remote Collection Engines functionality of the Summit WM Controller, Access Points and WM software solution. The Remote Collection Engines functionality is only available for the Summit WM Controller WM200/2000.

6 For the data collection engine:

- In the **Poll interval** box, type (in seconds) the interval that the Analysis Engine will poll the RF Data Collector to maintain connection status. The default is **30** seconds.
- In the **Poll retry count** box, type the number of times the Analysis Engine will attempt to poll the RF Data Collector to maintain connection status, before it stops sending requests. The default is **2** attempts.

7 Click **Add**. The IP address of the Data Collection Engine, with its Poll Interval and Poll Retry parameters is displayed in the list.

NOTE

For each remote RF Data Collection Engine defined here, you must:
*- Enable it by selecting the **Enable Summit Spy Analysis Engine** checkbox on the remote Summit WM Controller*
- Ensure that the controllers are routable by whatever means you use (for example, static routes, or OSPF).

8 To add a new collection engine, click **Add Collection Engine**.

9 Repeat steps 4 to 7.

10 To save your changes, click **Apply**.

Running Summit WM series Spy scans

The Summit WM series Spy feature allows you to view the following:

- Scan Groups
- Friendly APs
- AP Maintenance

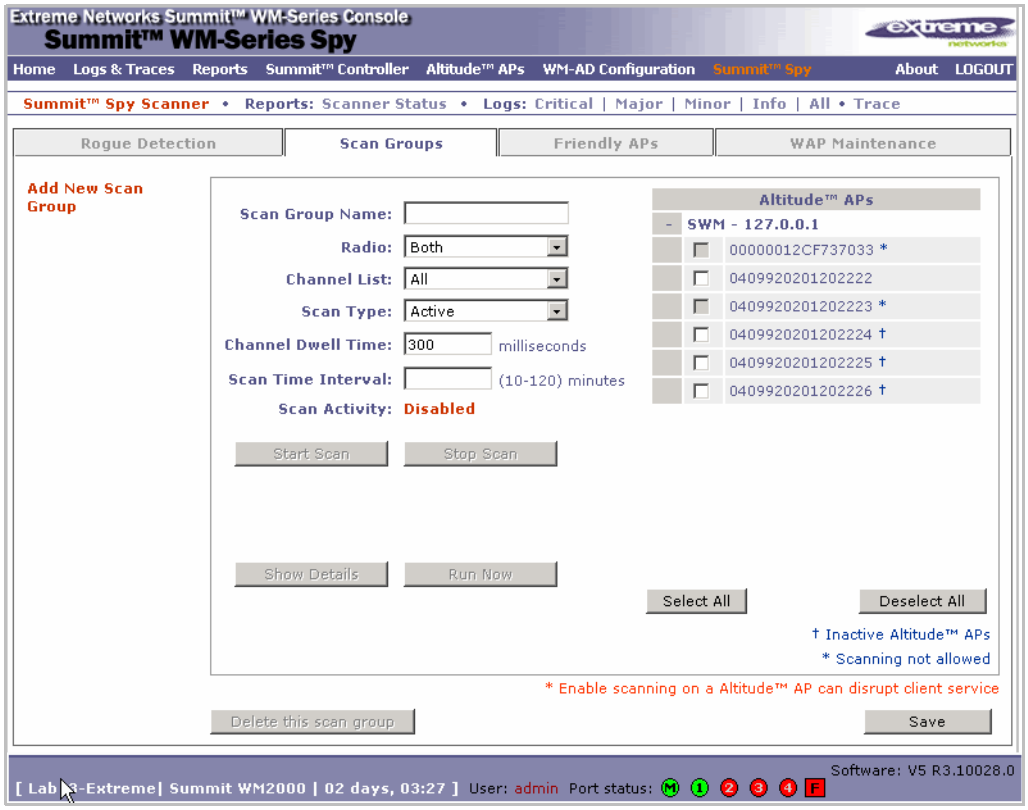
NOTE

A scan will not run on an inactive AP, even though it is displayed as part of the Scan Group. If it becomes active, it will be sent a scan request during the next periodic scan.

To run the Summit WM series Spy scan task mechanism:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Scan Groups** tab.



3 In the **Scan Group Name** box, type a unique name for this scan group.

4 In the **Altitude APs** list, select the checkbox corresponding to the Wireless APs you want included in the new scan group, which will perform the scan function.

NOTE

A Wireless AP can participate in only one Scan Group at a time. It is recommended that the Scan Groups represent geographical groupings of Wireless APs.

5 In the **Radio** drop-down list, click one of the following:

- **Both** - The 11a and 11b/g radios both perform the scan function.
- **11a** - Only the 11a radio performs the scan function.
- **11b/g** - Only the 11b/g radio performs the scan function.

6 In the **Channel List** drop-down list, click one of the following:

- **All** - Scanning is performed on all channels.
- **Current** - Scanning is performed on only the current channel.

7 In the **Scan Type** drop-down list, click one of the following:

- **Active** - The Wireless AP sends out ProbeRequests and waits for ProbeResponse messages from any access points.

- **Passive** - The Wireless AP listens for 802.11 beacons.

8 In the **Channel Dwell Time** box, type the time (in milliseconds) for the scanner to wait for a response from either 802.11 beacons in passive scanning, or ProbeResponse in active scanning.

9 In the **Scan Time Interval** box, type the time (in minutes) to define the frequency at which a Wireless AP within the Scan Group will initiate a scan of the RF space. The range is from one minute to 120 minutes.

10 To initiate a scan using the periodic scanning parameters defined above, click **Start Scan**.

11 To initiate an immediate scan that will run only once, click **Run Now**.

NOTE

*If necessary, you can stop a scan by clicking **Stop Scan**.*
A scan must be stopped before modifying any parameters of the Scan Group, or before adding or removing a Wireless AP from a Scan Group.

12 The **Scan Activity** box displays the current state of the scan engine.

13 To view a pop-up report showing the timeline of scan activity and scan results, click **Show Details**.

14 To save your changes, click **Save**.

Analysis engine overview

The Analysis engine relies on a database of known devices on the Controller, Access Points and Convergence Software system. The Analysis engine compares the data from the RF Data Collector with the database of known devices.

This database includes the following:

- **Altitude APs** - Registered with any Summit WM Controller with its RF Data Collector enabled and associated with the Analysis Engine on this Summit WM Controller.
- **Third-party APs** - Defined and assigned to a WM-AD.
- **Friendly APs** - A list created in the Summit WM series Spy user interface as potential rogue access points are designated by the administrator as Friendly.
- **Wireless devices** - Registered with any Summit WM Controller that has its RF Data Collector enabled and has been associated with the Analysis Engine on this Summit WM Controller.

The Analysis Engine looks for access points with one or more of the following conditions:

- **Unknown MAC address and unknown SSID** (critical alarm)
- **Unknown MAC, with a valid SSID** - a known SSID is being broadcast by the unknown access point (critical alarm)
- **Known MAC, with an unknown SSID** - a rogue may be spoofing a MAC address (critical alarm)
- **Inactive Wireless AP with valid SSID** (critical alarm)
- **Inactive Wireless AP with unknown SSID** (critical alarm)
- **Known Wireless AP with an unknown SSID** (major alarm)
- **In ad-hoc mode** (major alarm)

NOTE

In the current release, there is no capability to initiate a DoS attack on the detected rogue access point. Containment of a detected rogue requires an inspection of the geographical location of its Scan Group area, where its RF activity has been found.

Working with Summit WM series Spy scan results

When viewing the Summit WM series Spy scan results, you can delete individual or all of the access points from the scan results. You can also add access points from the scan results to the **Friendly AP** list.

To view Summit WM series Spy scan results:

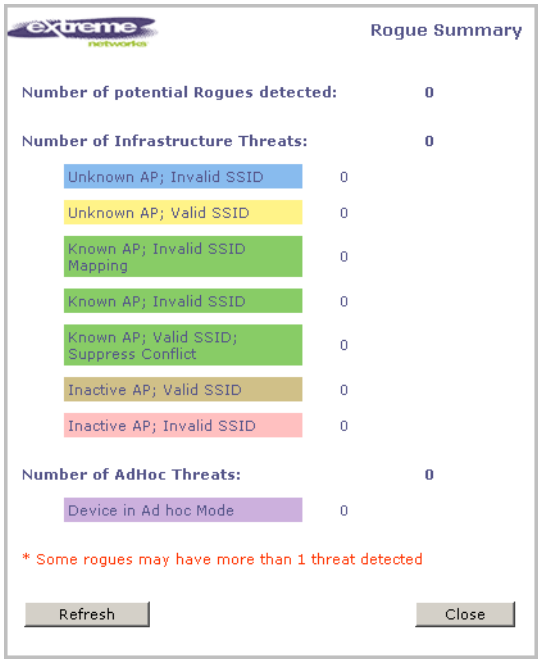
1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Rogue Detection** tab.

3 To modify the page's refresh rate, type a time (in seconds) in the **Refresh every __ seconds** box.

4 Click **Apply**. The new refresh rate is applied.

5 To view the Rogue Summary report, click **Rogue Summary**. The Rogue Summary report is displayed in a pop-up window.


Rogue Summary
Number of potential Rogues detected: 0
Number of Infrastructure Threats: 0
Unknown AP; Invalid SSID 0
Unknown AP; Valid SSID 0
Known AP; Invalid SSID Mapping 0
Known AP; Invalid SSID 0
Known AP; Valid SSID; Suppress Conflict 0
Inactive AP; Valid SSID 0
Inactive AP; Invalid SSID 0
Number of AdHoc Threats: 0
Device in Ad hoc Mode 0
* Some rogues may have more than 1 threat detected
Refresh
Close

6 To clear all detected rogue devices from the list, click **Clear Detected Rogues**.

NOTE

*To avoid the Summit WM series Spy's database becoming too large, it is recommended that you either delete Rogue APs or add them to the **Friendly APs** list, rather than leaving them in the **Rogue** list.*

To add an AP from the Summit WM series Spy scan results to the list of friendly APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Rogue Detection** tab.

3 To add a Wireless AP to the **Friendly APs** list, click **Add to Friendly List**. The AP is removed from this list and is displayed in the **Friendly AP Definitions** section of the **Friendly AP's** tab.

To delete an AP from the Summit WM series Spy scan results:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Rogue Detection** tab.

3 To delete a specific AP from the Summit WM series Spy scan results, click the corresponding **Delete** button. The AP is removed from the list.

4 To clear all rogue access points from the Summit WM series Spy scan results, click **Clear Detected Rogues**. All APs are removed from the list.

Working with friendly APs

To view the friendly APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Friendly APs** tab.

To add friendly APs manually:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Friendly APs** tab.

3 To add friendly access points manually to the **Friendly AP Definitions** list, type the following:

- MAC Address - Specifies the MAC address for the friendly AP
- SSID - Specifies the SSID for the friendly AP
- Channel - Specifies the current operating channel for the friendly AP
- **Description** - Specifies a brief description for the friendly AP

4 Click **Add**. The new access point is displayed in the list above.

To delete a friendly AP:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Friendly APs** tab.

3 In the **Friendly AP Definitions** list, click the access point you want to delete.

4 Click **Delete**. The selected access point is removed from the **Friendly AP Definitions** list.

5 To save your changes, click **Save**.

To modify a friendly AP:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Friendly APs** tab.

3 In the **Friendly AP Definitions** list, click the access point you want to modify.

4 Modify the access point by making the appropriate changes.

5 To save your changes, click **Save**.

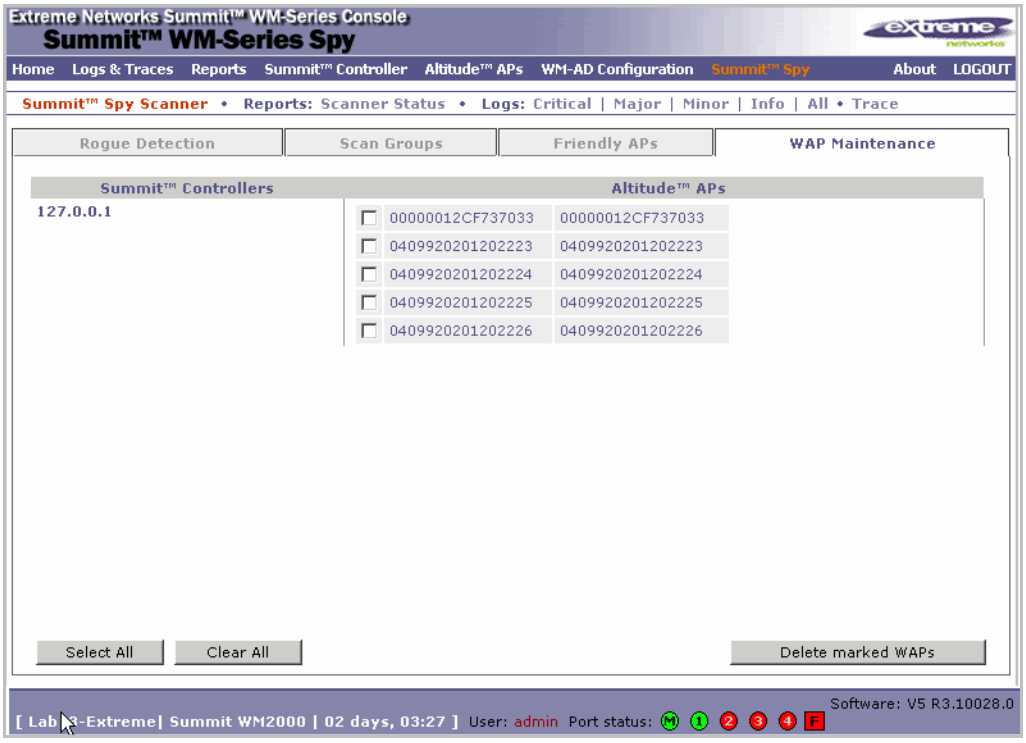
Maintaining the Summit WM series Spy list of APs

To maintain the Altitude APs:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **WAP Maintenance** tab. Inactive APs and known third-party APs are displayed.

3 Select the applicable APs.



4 To delete the selected APs, click **Delete marked WAPs**.

NOTE

The selected APs are deleted from the Summit WM series Spy database, not from the Summit WM Controller database. You can delete the APs from the Summit WM Controller database after you delete them from the ***Altitude AP Configuration Access Approval*** *page of the corresponding RF Data Collector Engine. You can also delete the selected third-party APs if they are removed from the corresponding WM-AD in the RF Collector Engine, or if that WM-AD has been deleted from the WM-AD list.*

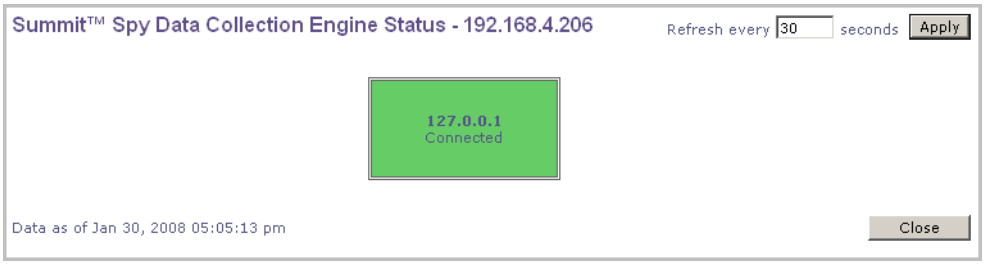
Viewing the Scanner Status report

When the Summit WM series Spy is enabled, you can view a report on the connection status of the RF Data Collector Engines with the Analysis Engine.

To view the Summit WM series Spy scanner engine status display:

1 From the main menu, click **Summit Spy**. The **Summit Spy** page is displayed.

2 Click the **Reports: Scanner Status**. The Scanner Status report is displayed, as shown in the example below.



The boxes display the IP address of the Data Collector engine. The status of the Data Collector engine is indicated by one of the following colors:

- **Green** - The Analysis Engine has connection with the Data Collector on that Summit WM Controller.
- **Yellow** - The Analysis Engine has connected to the communication system of the other controller, but has not synchronized with the Data Collector. Ensure that the Data Collector is running on the remote controller.
- **Red** - The Analysis Engine is aware of the Data Collector and attempting connection.

If no box is displayed, the Analysis Engine is not attempting to connect with that Data Collector Engine.

NOTE

If the box is displayed red and remains red, ensure your IP address is correctly set up to point to an active controller. If the box remains yellow, ensure the Data Collector is running on the remote controller.

10 Working with reports and displays

This chapter describes the various reports and displays available in the Summit WM Controller, Access Points, and WM software system, including:

- "Viewing the displays" on page 273
- "Viewing reports" on page 285
- "Call Detail Records (CDRs)" on page 288

Viewing the displays

The following displays are available in the Summit WM Controller, Access Points, and WM software system:

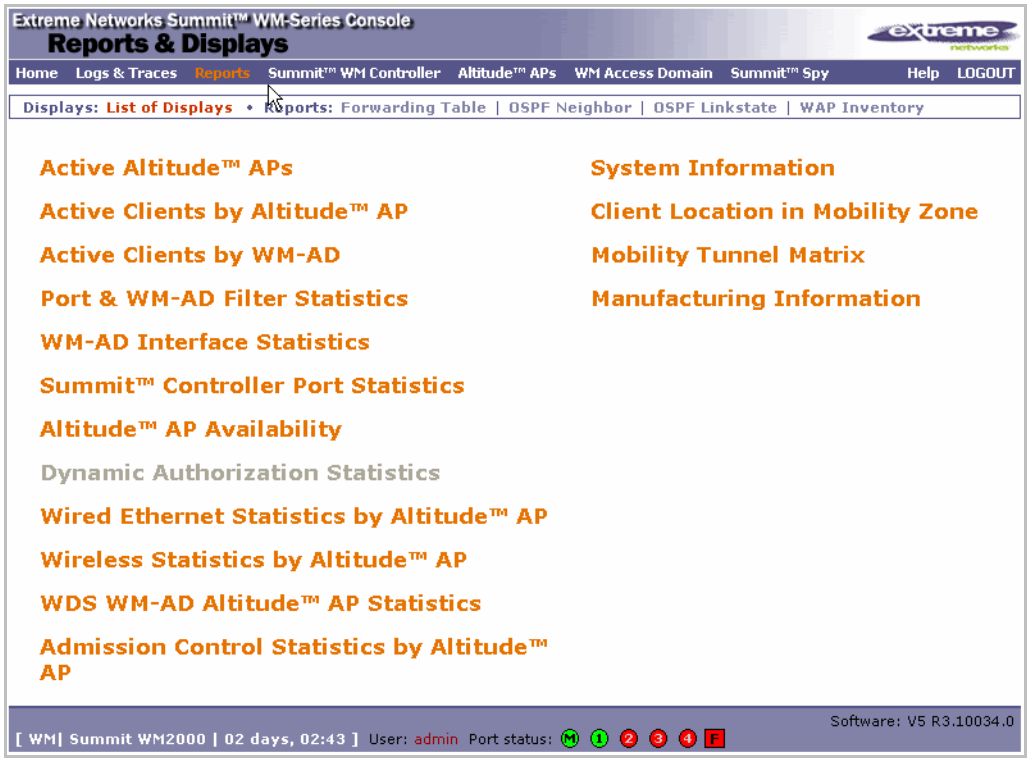
- Active Altitude APs
- Active Clients by Altitude AP
- Active Clients by WM-AD
- Port & WM-AD Filter Statistics
- WM-AD Interface Statistics
- Summit Controller Port Statistics
- Altitude AP Availability
- Dynamic Authorization Statistics
- Wired Ethernet Statistics by Altitude AP
- Wireless Statistics by Altitude AP
- WDS WM-AD Altitude AP Statistics
- Admission Control Statistics by Altitude AP
- System Information
- Manufacturing Information
- Client Location in Mobility Zone
- Mobility Tunnel Matrix

NOTE

*The **Client Location in Mobility Zone** and **Mobility Tunnel Matrix** displays only appear if the mobility manager function has been enabled for the controller.*

To view reports and displays:

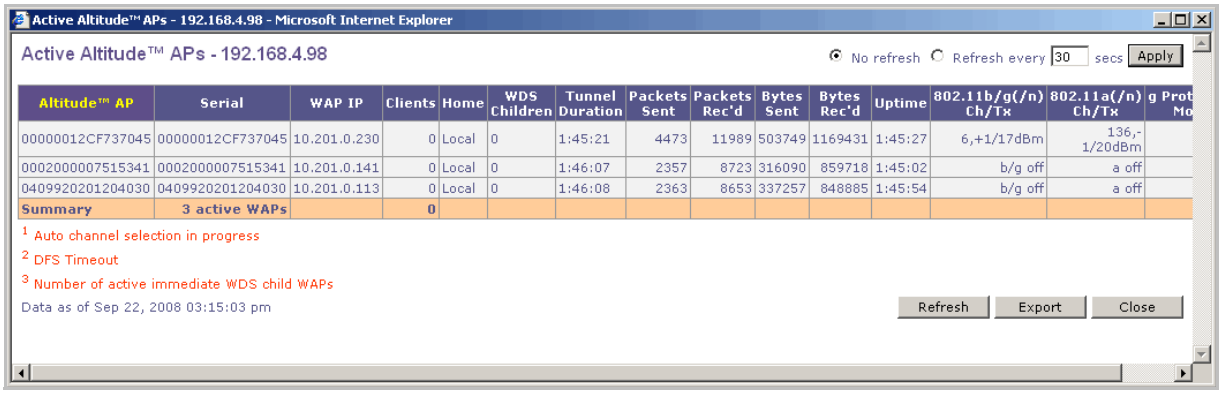
1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.


Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Port & WM-AD Filter Statistics
WM-AD Interface Statistics
Summit™ Controller Port Statistics
Altitude™ AP Availability
Dynamic Authorization Statistics
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
WDS WM-AD Altitude™ AP Statistics
Admission Control Statistics by Altitude™ AP
System Information
Client Location in Mobility Zone
Mobility Tunnel Matrix
Manufacturing Information
Software: V5 R3.10034.0
[WM| Summit WM2000 | 02 days, 02:43] User: admin Port status:

NOTE

*The **Client Location in Mobility Zone** and **Mobility Tunnel Matrix** displays only appear if the mobility manager function has been enabled for the controller.*

2 In the **List of Displays**, click the display you want to view (some examples will follow):


Active Altitude™ APs - 192.168.4.98 - Microsoft Internet Explorer
Active Altitude™ APs - 192.168.4.98
No refresh Refresh every 30 secs Apply
Altitude™ AP | Serial | WAP IP | Clients | Home | WDS Children | Tunnel Duration | Packets Sent | Packets Rec'd | Bytes Sent | Bytes Rec'd | Uptime | 802.11b/g(/n) Ch/Tx | 802.11a(/n) Ch/Tx | g Prot Mo
00000012CF737045 | 00000012CF737045 | 10.201.0.230 | 0 | Local | 0 | 1:45:21 | 4473 | 11989 | 503749 | 1169431 | 1:45:27 | 6,+1/17dBm | 136,-1/20dBm
0002000007515341 | 0002000007515341 | 10.201.0.141 | 0 | Local | 0 | 1:46:07 | 2357 | 8723 | 316090 | 859718 | 1:45:02 | b/g off | a off
0409920201204030 | 0409920201204030 | 10.201.0.113 | 0 | Local | 0 | 1:46:08 | 2363 | 8653 | 337257 | 848885 | 1:45:54 | b/g off | a off
Summary | 3 active WAPs | 0
1 Auto channel selection in progress
2 DFS Timeout
3 Number of active immediate WDS child WAPs
Data as of Sep 22, 2008 03:15:03 pm
Refresh Export Close

NOTE

*Statistics are expressed in relation to the AP. Therefore, **Packets Sent** means the AP has sent that data to a client and **Packets Rec'd** means the AP has received packets from a client.*

Viewing the Wireless AP availability display

Summit WM 100/1000

The report uses the **Color Legend** to indicate the tunnel state. The description of the colors codes in the legend is given below:

- **Green** - Altitude AP has established an active tunnel.
- **Blue** - Altitude AP has established a backup tunnel.

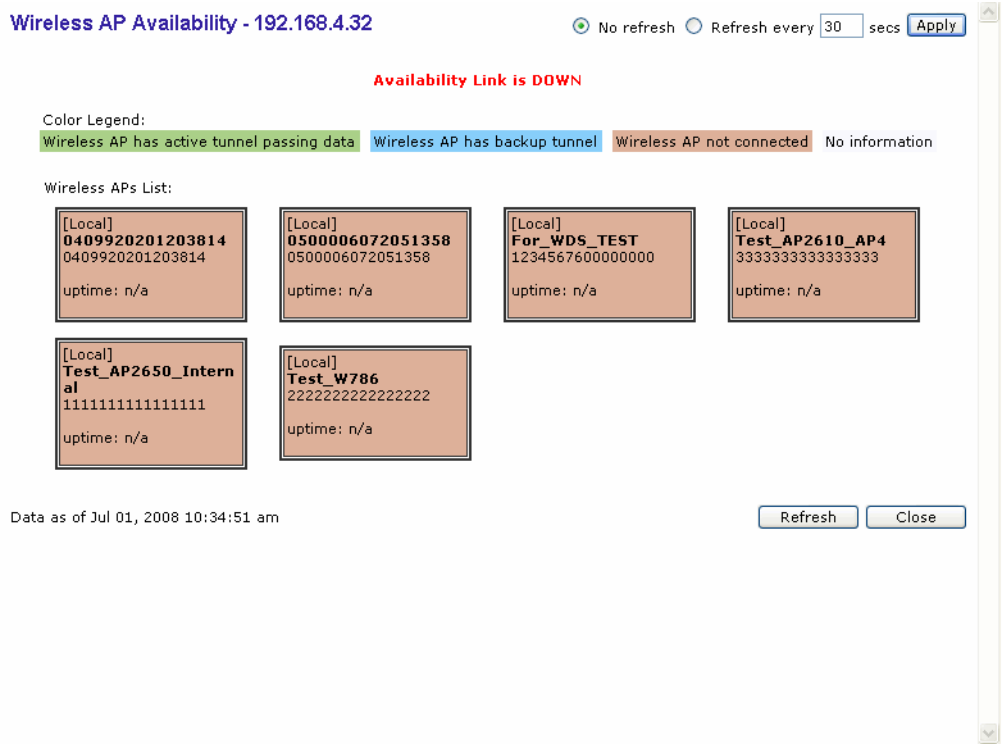
NOTE

The Blue color is not applicable when the controller is paired in availability. It is applicable only when the controller is paired in session availability with fast failover enabled. Since the Summit WM Controller 100/1000 does not support fast failover and session availability, you must ignore the Blue color in the legend.

- **Red** - Wireless AP is not connected.

In the report, each Altitude AP is represented by a box.

- The label, **Foreign** or **Local**, indicates whether the Altitude AP is local or foreign on the Summit WM Controller.



Summit WM 200/2000

In session availability, the Wireless Availability report displays the state of both the tunnels - active tunnel and backup tunnel - on both the primary and secondary Summit WM Controllers.

The report uses the **Color Legend** to indicate the tunnel state. The description of the colors codes in the legend is given below:

- **Green** - Altitude AP has established an active tunnel.
- **Blue** - Altitude AP has established a backup tunnel.
- **Red** - Altitude AP is not connected.

In the report, each Altitude AP is represented by a box.

- The label, **Foreign** or **Local,** indicates whether the Altitude AP is local or foreign on the Summit WM Controller.
- The color in the upper pane of the box represents the state of the tunnel that is established to the current Summit WM Controller.

NOTE

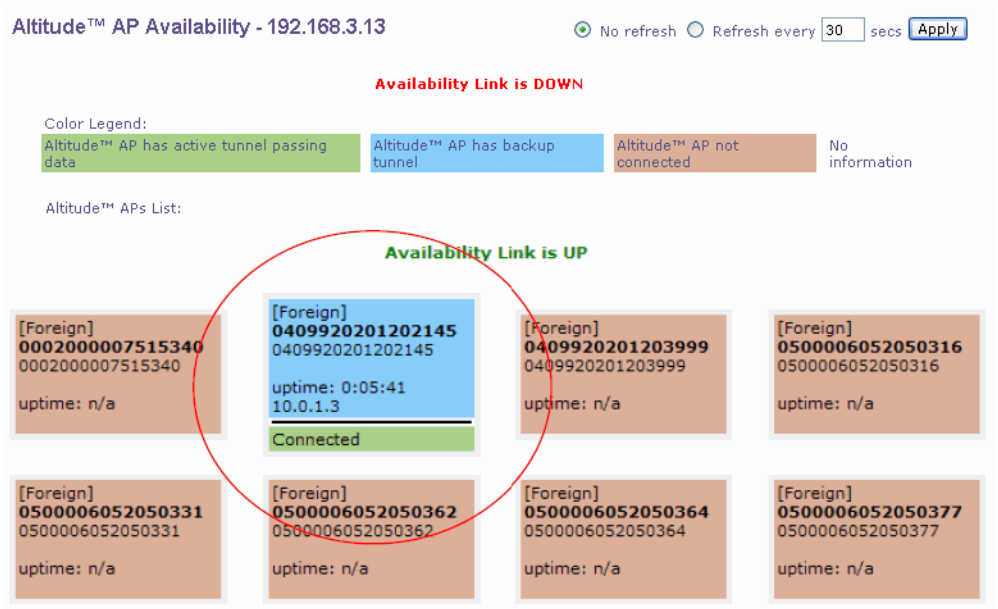
The current Summit WM Controller is the one on which the Altitude AP Availability report is viewed.

- The color in the lower pane of the box represents the state of the tunnel that is established with the other Summit WM Controller.

For the ease of understanding, take the example of the following scenario:

- WM1 and WM2 are paired in session availability
- An Altitude AP has established an active tunnel to WM1.
- The same Altitude AP has established a backup tunnel to WM2.

If you open the Altitude AP Availability report on WM2, the report will appear as follows:



In the above screen shot, the Altitude AP, which is circled, has established backup tunnel to the foreign (secondary) Summit WM Controller, and active tunnel to the local (Primary) Summit WM Controller.

Viewing statistics for Wireless APs

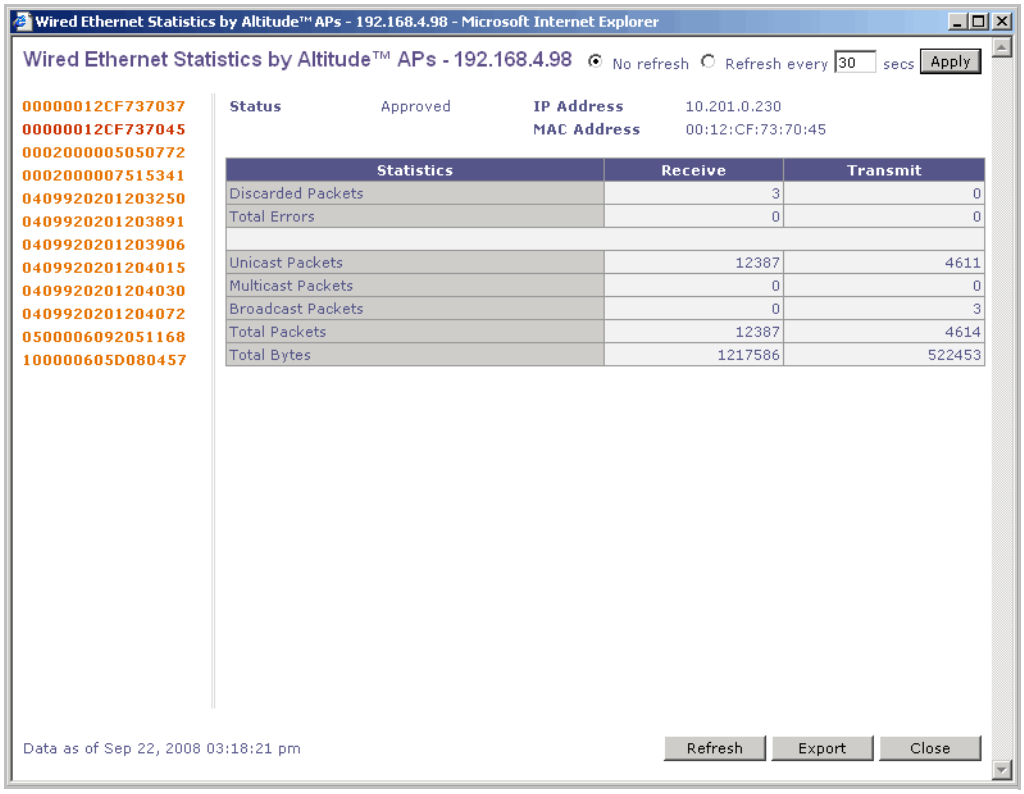
- Several displays are snapshots of activity at that point in time on a selected Wireless AP:
- Wired Ethernet Statistics by Wireless AP
- Wireless Statistics by Wireless AP
- Active Clients by Altitude AP
- WDS WM-AD Altitude AP Statistics
- Admission Control Statistics by Altitude AP

The statistics displayed are those defined in the 802.11 MIB, in the IEEE 802.11 standard.

To view wired Ethernet statistics by Wireless AP:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **Wired Ethernet Statistics by Altitude AP** display option. The **Wired Ethernet Statistics by Altitude APs** display opens in a new browser window.

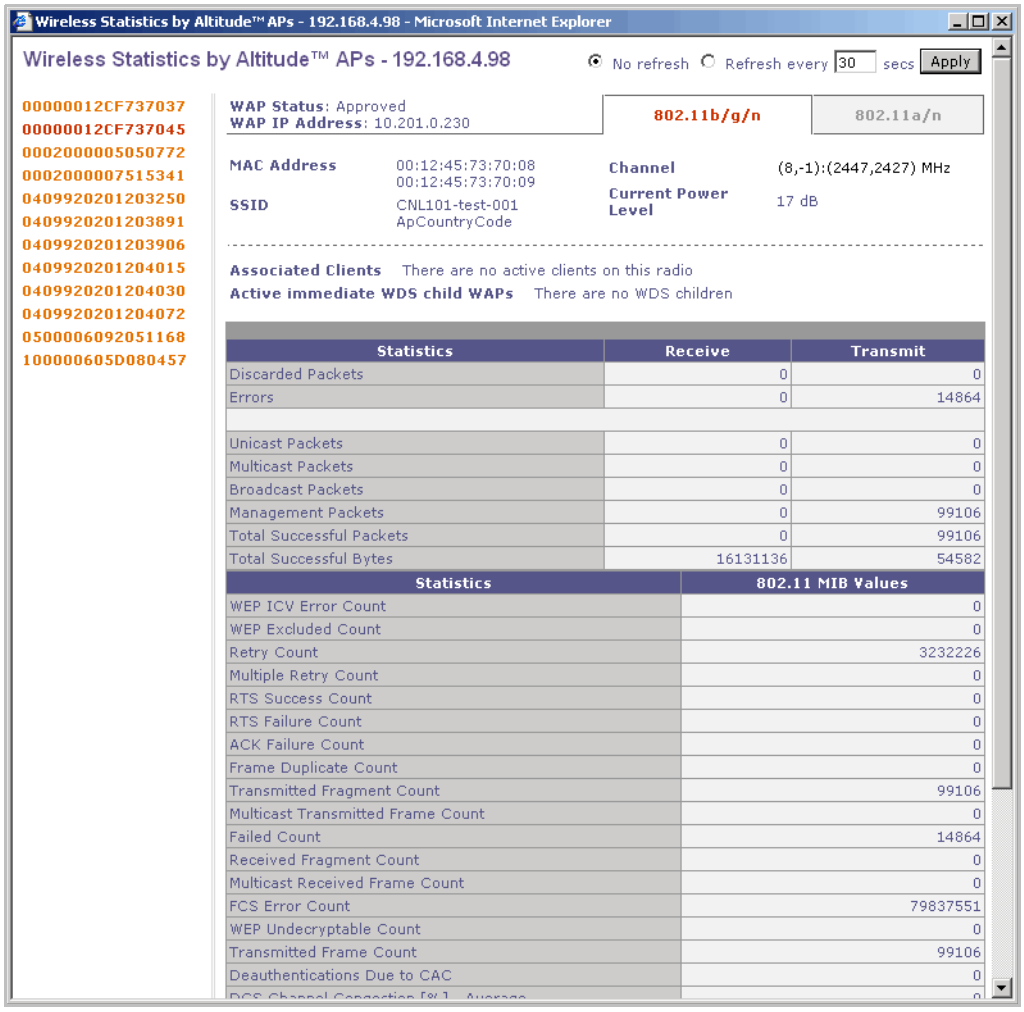


3 In the **Wired Ethernet Statistics by Altitude APs** display, click a registered Wireless AP to display its information.

To view Wireless Statistics by Altitude AP:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **Wireless Statistics by Altitude AP** display option. The **Wireless Statistics by Altitude APs** display opens in a new browser window.



3 In the **Wireless Statistics by Altitude APs** display, click a registered Wireless AP to display its information.

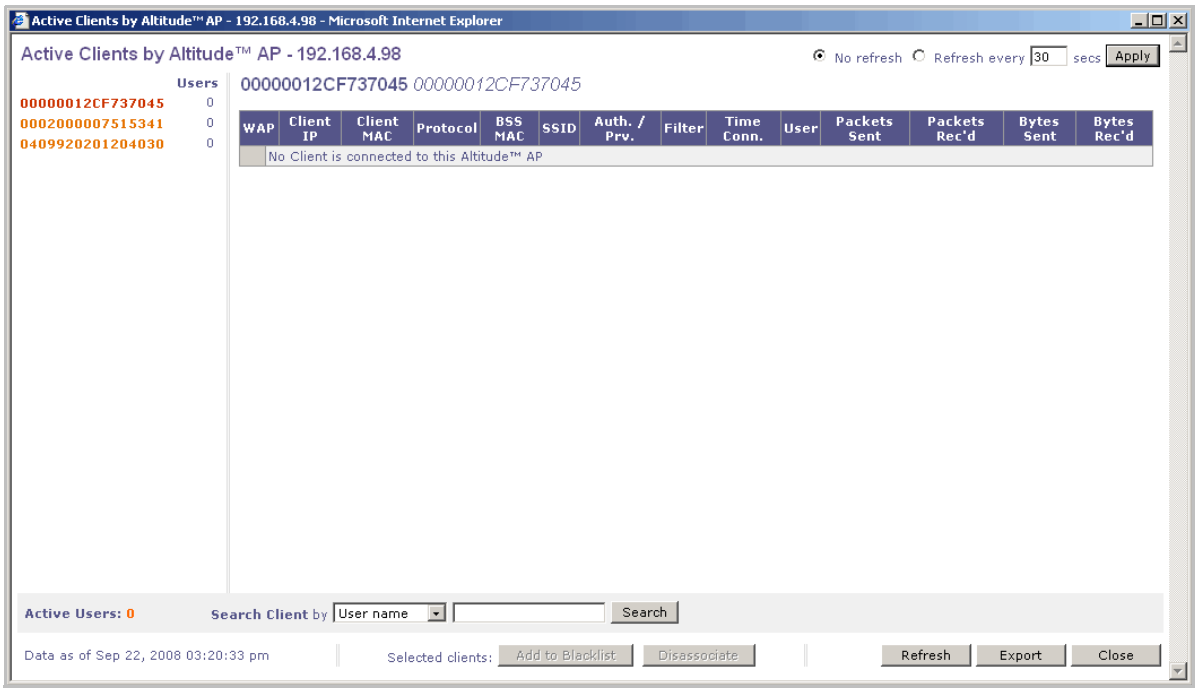
4 Click the appropriate tab to display information for each radio on the Wireless AP.

5 To view information on the associated clients, click **View Client**. The **Associated Clients** display opens in a new browser window.

To view Active Clients by Altitude AP statistics:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **Active Clients by Altitude APs** display option. The **Active Clients by Altitude APs** display opens in a new browser window.

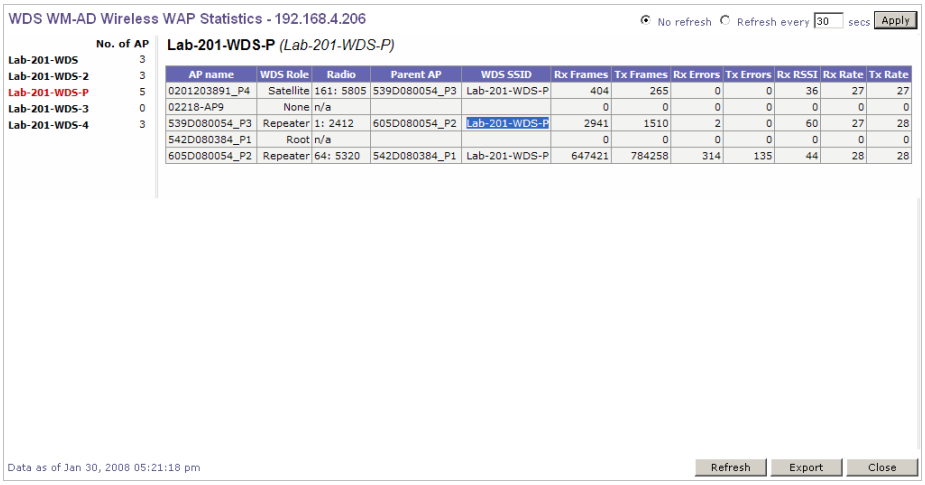


- Statistics are expressed in respect of the AP. Therefore, **Packets Sent** means the AP has sent that data to a client and **Packets Rec'd** means the AP has received packets from a client.
- If the client is authenticated, a green check mark icon is displayed in the first column of the display.
- **Time Conn** is the length of time that a client has been on the system, not just on an AP. If the client roams from one AP to another, the session stays, therefore **Time Conn** does not reset.
- A client is displayed as soon as the client connects (or after refresh of page). The client disappears as soon as it times out.

To view WDS Wireless AP Statistics:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **WDS Altitude AP Statistics** display option. The **WDS Altitude AP Statistics** display opens in a new browser window.


WDS WM-AD Wireless WAP Statistics - 192.168.4.206
No refresh
Refresh every 30 secs
Apply
No. of AP
Lab-201-WDS 3
Lab-201-WDS-2 3
Lab-201-WDS-P 5
Lab-201-WDS-3 0
Lab-201-WDS-4 3
Lab-201-WDS-P (Lab-201-WDS-P)
AP name | WDS Role | Radio | Parent AP | WDS SSID | Rx Frames | Tx Frames | Rx Errors | Tx Errors | Rx RSSI | Rx Rate | Tx Rate
0201203891_P4 | Satellite | 161: 5805 | 539D080054_P3 | Lab-201-WDS-P | 404 | 265 | 0 | 0 | 36 | 27 | 27
02218-AP9 | None | n/a | | | 0 | 0 | 0 | 0 | 0 | 0 | 0
539D080054_P3 | Repeater | 1: 2412 | 605D080054_P2 | Lab-201-WDS-P | 2941 | 1510 | 2 | 0 | 60 | 27 | 28
542D080384_P1 | Root | n/a | | | 0 | 0 | 0 | 0 | 0 | 0 | 0
605D080054_P2 | Repeater | 64: 5320 | 542D080384_P1 | Lab-201-WDS-P | 647421 | 784258 | 314 | 135 | 44 | 28 | 28
Data as of Jan 30, 2008 05:21:18 pm
Refresh
Export
Close

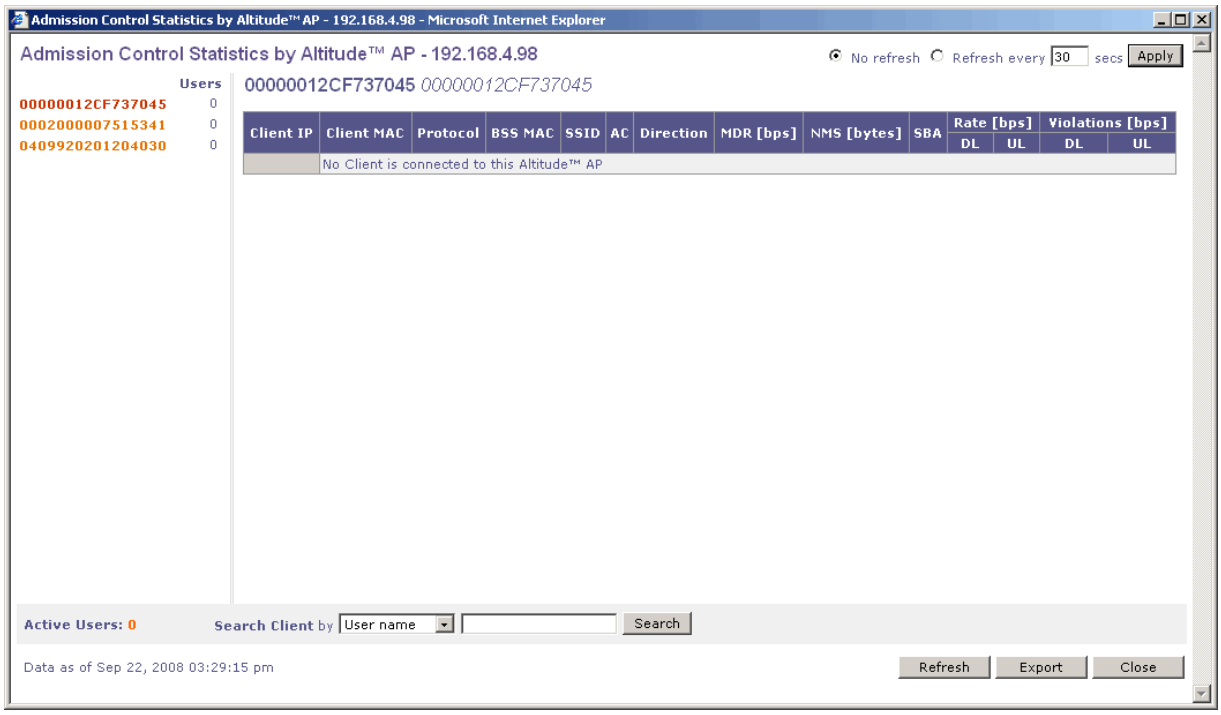
NOTE

*RSSI value on the **WDS WM-AD Wireless AP Statistics** display denotes the signal strength. The minimum value is 1 and maximum value is 60. The higher the RSSI value, the stronger the received signal.*

To view Admission Control Statistics by Wireless AP:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **Admission Control Statistics by Wireless AP** display option. The **Admission Control Statistics by Wireless AP** display opens in a new browser window.



3 In the **Admission Control Statistics by Altitude AP** display, click a registered Altitude AP to display its information:

4 The Admission Control Statistics by Altitude AP lists the TSPEC statistics associated with this Altitude AP:

- **AC** - Access class where TSPEC is applied,
- **Direction** - Uplink, Downlink or Bidirectional,
- **MDR** - Mean Data Rate
- **NMS** - Nominal Packet Size
- **SBA** - Surplus Bandwidth (ratio)

The following two statistics are of the measured traffic:

- **Rate** - Rate in 30 second intervals (uplink and downlink)
- **Violation** - Number of bits in excess in the last 30 seconds (uplink and downlink)

Viewing the System Information and Manufacturing Information displays

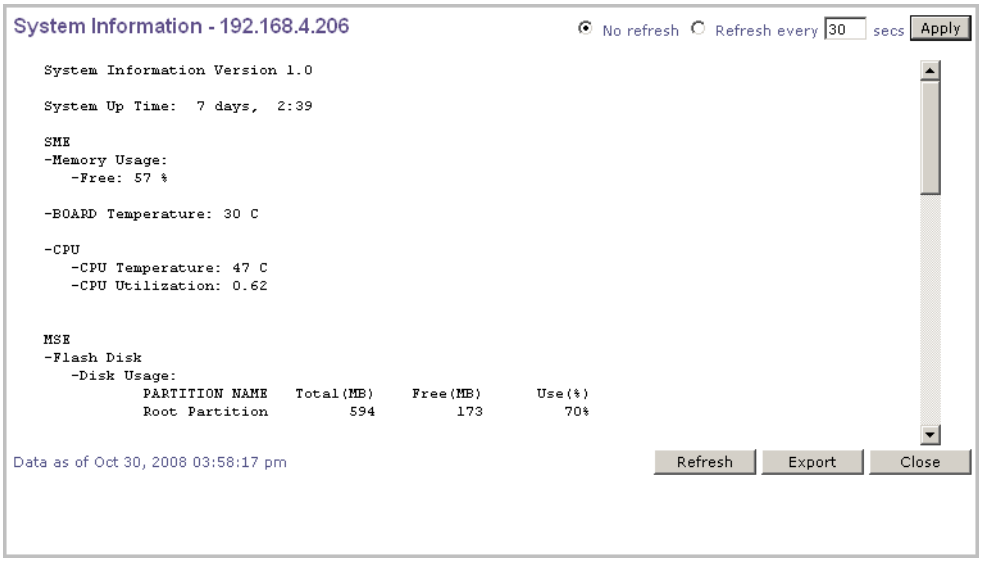
System Information - Displays system information including memory usage and CPU and board temperatures.

Manufacturing Information - Displays manufacturing information including the card serial number and CPU type and frequency.

To view system information:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

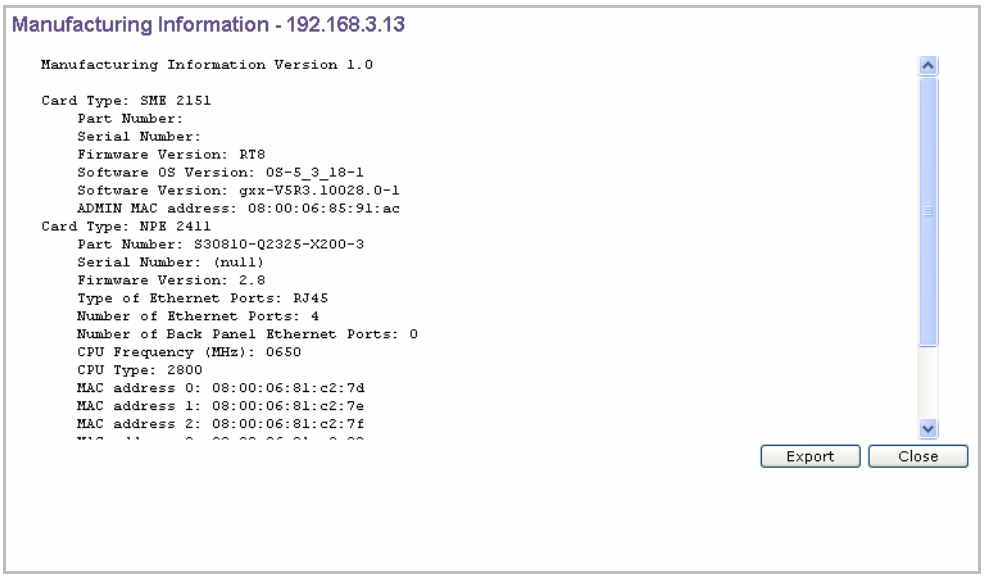
2 Click the **System Information** display option. The **System Information** display opens in a new browser window.



To view manufacturing information:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the **Manufacturing Information** display option. The **Manufacturing Information** display opens in a new browser window.



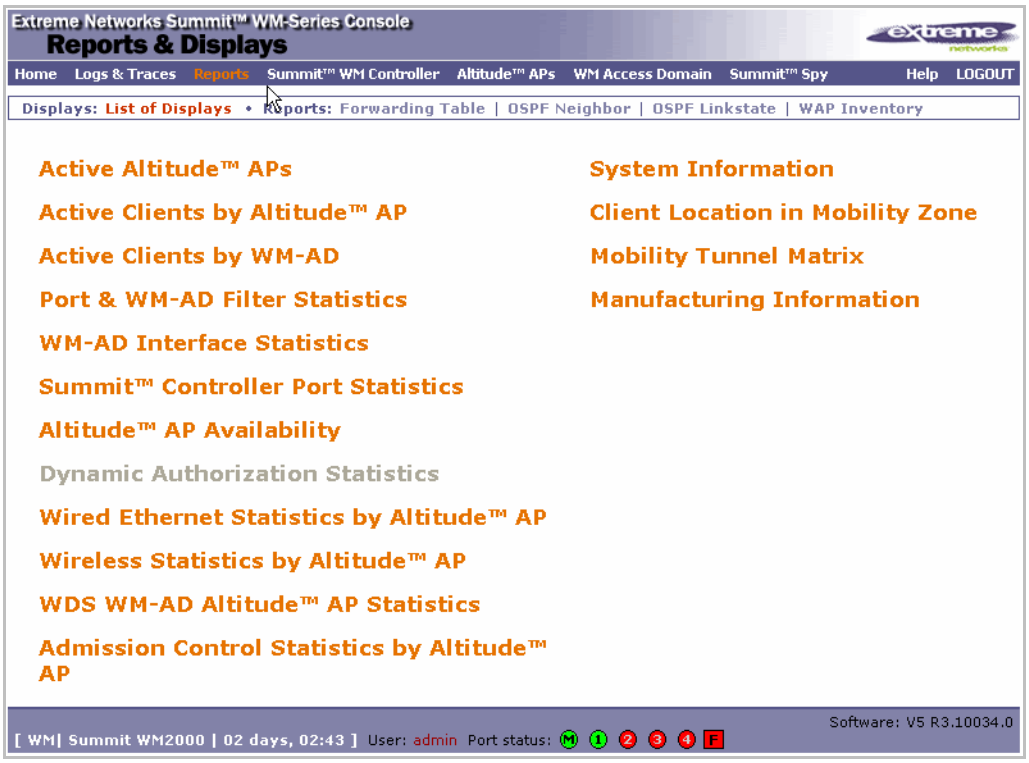
NOTE

In the latest models of the Summit WM 200/2000 Controller, the IXP2800 Network Processor in the NPE Card has been replaced by the new IXP2805 Network Processor. Consequently, the Manufacturing Information in all such latest models displays CPU Type as 2805.

Viewing displays for the mobility manager

When a Summit WM Controller has been configured as a mobility manager, two additional displays appear as options on the **Reports & Displays** page:

- **Client Location in Mobility Zone** - Displays the active wireless clients and their status
- **Mobility Tunnel Matrix** - Displays a cross-connection view of the state of inter-controller tunnels, as well as relative loading for user distribution across the mobility domain


Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Active Altitude™ APs
Active Clients by Altitude™ AP
Active Clients by WM-AD
Port & WM-AD Filter Statistics
WM-AD Interface Statistics
Summit™ Controller Port Statistics
Altitude™ AP Availability
Dynamic Authorization Statistics
Wired Ethernet Statistics by Altitude™ AP
Wireless Statistics by Altitude™ AP
WDS WM-AD Altitude™ AP Statistics
Admission Control Statistics by Altitude™ AP
System Information
Client Location in Mobility Zone
Mobility Tunnel Matrix
Manufacturing Information
Software: V5 R3.10034.0
[WM| Summit WM2000 | 02 days, 02:43] User: admin Port status: M 1 2 3 4 F

To view mobility manager displays:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 Click the appropriate mobility manager display:

- Client Location in Mobility Zone
- Mobility Tunnel Matrix

The colored status indicates the following:

- **Green** - The mobility manager is in communication with an agent and the data tunnel has been successfully established.

- **Yellow** - The mobility manager is in communication with an agent but the data tunnel is not yet successfully established.
- **Red** - The mobility manager is not in communication with an agent and there is no data tunnel.

Client Location in Mobility Zone

You can do the following:

- Sort this display by home or foreign controller
- Search for a client by MAC address, user name, or IP address, and typing the search criteria in the box
- Define the refresh rates for this display
- Export this information as an xml file

Mobility Tunnel Matrix

- Provides connectivity matrix of mobility state
- Provides a view of:
  - Tunnel state
  - If a tunnel between controllers is reported down, it is highlighted in red
  - If only a control tunnel is present, it is highlighted in yellow
  - If data and control tunnels are fully established, it is highlighted in green
  - Tunnel Uptime
  - Number of clients roamed (Mobility loading)
  - Local controller loading
  - Mobility membership list

A Summit WM Controller is only removed from the mobility matrix if it is explicitly removed by the administrator from the Mobility permission list. If a particular link between controllers, or the controller is down, the corresponding matrix connections are identified in red color to identify the link.

The Active Clients by WM-AD report for the controller on which the user is home (home controller) will display the known user characteristics (IP, statistics, etc.). On the foreign controller, the Clients by WM-AD report does not show users that have roamed from other controllers, since the users remain associated with the home controller's WM-AD.

The Active Clients by AP report on each controller will show both the loading of local and foreign users (users roamed from other controllers) that are taking resources on the AP.

NOTE

Although you can set the page refresh period less than 30 seconds, the page will not be refreshed quicker than 30 seconds. The page will be refreshed according to the value you set only if you set the value above 30 seconds.

Viewing reports

The following reports are available in the Summit WM Controller, Access Points, and WM software system:

- Forwarding Table (routes defined on the **Routing Protocols** pages)
- OSPF Neighbor (if OSPF is enabled on the **Routing Protocols** pages)
- OSPF Linkstate (if OSPF is enabled on the **Routing Protocols** pages)
- AP Inventory (a consolidated summary of Wireless AP setup)

To view reports:

1 From the main menu, click **Reports & Displays**. The **Reports & Displays** page is displayed.

2 In the **Reports** list, click the report you want to view:

- Forwarding Table
- OSPF Neighbor
- OSPF Linkstate
- AP Inventory

NOTE

*The **AP Inventory** report opens in a new browser window. All other reports appear in the current browser window.*

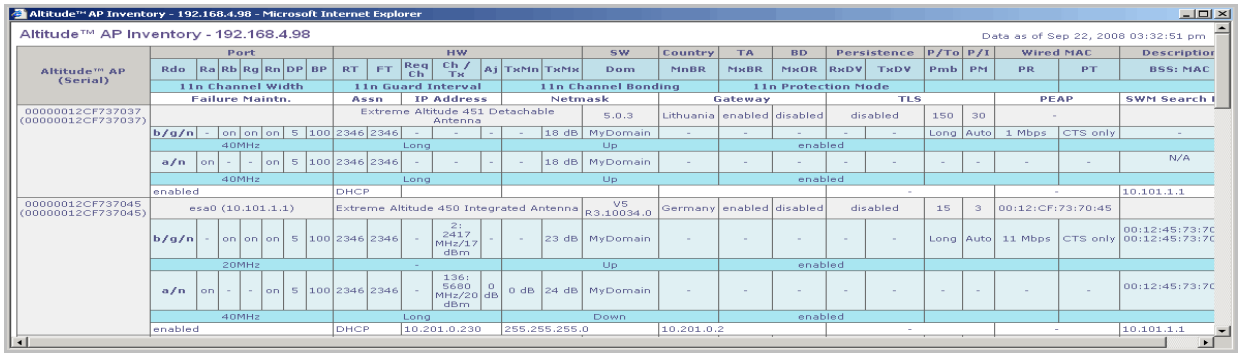
The following is an example of a **Forwarding Table** report:

Extreme Networks Summit™ WM-Series Console
Reports & Displays
Home Logs & Traces Reports Summit™ WM Controller Altitude™ APs WM Access Domain Summit™ Spy Help LOGOUT
Displays: List of Displays • Reports: Forwarding Table | OSPF Neighbor | OSPF Linkstate | WAP Inventory
Route # Destination Netmask Gateway Interface Type Status
1 0.0.0.0 0.0.0.0 10.13.0.2 esa0 OSPF Active
2 1.1.1.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
3 2.2.2.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
4 7.7.7.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
5 8.8.8.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
6 10.1.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
7 10.1.1.0 255.255.255.0 esa8 Connected Active
8 10.1.99.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
9 10.2.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
10 10.3.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
11 10.4.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
12 10.5.0.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
13 10.5.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
14 10.5.16.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
15 10.5.32.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
16 10.5.48.0 255.255.240.0 10.13.0.2 esa0 OSPF Active
17 10.6.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
18 10.7.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
19 10.8.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
20 10.9.0.0 255.255.255.0 10.13.0.2 esa0 OSPF Active
Export
Refresh
[Lab13-Extreme| Summit WM2000 | 02 days, 21:58] User: admin Port status: M 1 2 3 4 F
Software: V5 R3.10028.0

NOTE

If you open only automatically refreshed reports, the Web management session timer will not be updated or reset. Your session will eventually timeout.

The following is an example of the AP Inventory report:



Altitude™ AP Inventory - 192.168.4.98 - Microsoft Internet Explorer

Altitude™ AP Inventory - 192.168.4.98

Data as of Sep 22, 2008 03:32:51 pm

Altitude™ AP (Serial)	Port						HW							SW	Country	TA	BD	Persistence		P/To	P/I	Wired MAC		Description
	Rdo	Ra	Rb	Rg	Rn	DP	BP	RT	FT	Req Ch	Ch / Tx	Aj	TxMn	TxMx	Dom	MnBR	MxBR	MxOR	RxDV	TxDV	Pmb	PM	PR	PT	BSS: MAC
	11n Channel Width							11n Guard Interval					11n Channel Bonding			11n Protection Mode								
	Failure Maintn.							Assn	IP Address				Netmask			Gateway			TLS				PEAP		SWM Search I
00000012CF737037 (00000012CF737037)								Extreme Altitude 451 Detachable Antenna							5.0.3	Lithuania	enabled	disabled	disabled		150	30	-		
	b/g/n	-	on	on	on	5	100	2346	2346	-	-	-	-	18 dB	MyDomain	-	-	-	-	-	Long	Auto	1 Mbps	CTS only	-
	40MHz							Long					Up			enabled									
	a/n	on	-	-	on	5	100	2346	2346	-	-	-	-	18 dB	MyDomain	-	-	-	-	-	-	-	-	-	N/A
	40MHz							Long					Up			enabled									
	enabled							DHCP											-				-		10.101.1.1
00000012CF737045 (00000012CF737045)	esa0 (10.101.1.1)							Extreme Altitude 450 Integrated Antenna							V5 R3.10034.0	Germany	enabled	disabled	disabled		15	3	00:12:CF:73:70:45		
	b/g/n	-	on	on	on	5	100	2346	2346	-	2: 2417 MHz/17 dBm	-	-	23 dB	MyDomain	-	-	-	-	-	Long	Auto	11 Mbps	CTS only	00:12:45:73:70 00:12:45:73:70
	20MHz							-					Up			enabled									
	a/n	on	-	-	on	5	100	2346	2346	-	136: 5680 MHz/20 dBm	0 dB	0 dB	24 dB	MyDomain	-	-	-	-	-	-	-	-	-	00:12:45:73:70
	40MHz							Long					Down			enabled									
	enabled							DHCP	10.201.0.230				255.255.255.0			10.201.0.2			-				-		10.101.1.1

The following is a description of the column names and abbreviations found in the **AP Inventory** report:

- **Rdo** - Radio
- **Ra** - 802.11a radio. The data entry for an Wireless AP indicates whether the **11a radio** is on or off.
- **Rb** - 802.11b protocol enabled. Possible values are **on** or **off**.
- **Rg** - 802.11g protocol enabled. Possible values are **on** or **off**.
- **Rn** - 802.11n protocol enabled. Possible values are **on** or **off**.
- **DP** - DTIM period
- **BP** - Beacon Period
- **SRL** - Short Retry Limit
- **LRL** - Long Retry Limit
- **RT** - RTS Threshold
- **FT** - Fragmentation Threshold
- **Ch** - Channel served by the corresponding radio.
- **PL** - Power Level (Defined in the Wireless AP radio properties pages.)
- **BR** - Basic Rate (Only applies to Wireless APs running 3.1 or earlier.)
- **ORS** - Operational Rate Set (Only applies to Wireless APs running 3.1 or earlier.)
- **MnBR** - Minimum Basic Rate (For more information, see the Wireless AP radio configuration tabs.)
- **MxBR** - Maximum Basic Rate
- **MxOR** - Maximum Operational Rate
- **RxDV** - Receive Diversity
- **TxDV** - Tx Diversity
- **Pmb** - Preamble (long, short)
- **PM** - Protection Mode
- **PR** - Protection Rate
- **PT** - Protection Type

- **BSS** - Basic Service Set
- **MAC** - MAC address
- **BSS: MAC** - Also called BSSID, this is the MAC address of a (virtual) wireless interface on which the Wireless AP serves a BSS/WM-AD. There could be 8 per radio.
- **Port** - Ethernet Port and associated IP address of the interface on the Summit WM Controller through which the Wireless AP communicates.
- **HW** - Hardware version of the Wireless AP.
- **SW** - Software version executing on the Wireless AP.
- **TA** - Telnet access (enabled or disabled).
- **BD** - Broadcast disassociation (enabled or disabled). If enabled, whenever the Wireless AP is going offline in a controlled fashion it will send the disassociation frame to all its clients as a broadcast.
- **DV** - Diversity
- **P/To** - Poll timeout. If polling is enabled, a numeric value.
- **P/I** - Poll interval. If polling is enabled, a numeric value.
- **Wired MAC** - The physical address of the Wireless AP's wired Ethernet interface.
- **Description** - As defined on the **AP Properties** page.
- **Failure Maintn.** - Maintain MU sessions on Wireless AP when the Wireless AP loses the connection to the Summit WM Controller.
- **Assn** - Assignment (address assignment method)
- **Static Cfg** - Wireless AP's IP address if statically configured (same as the **Static Values** radio button on the **AP Static Configuration** page).
- **Static Cfg IP** - Statically Configured IP. If the Wireless AP's IP address is configured statically, the IP address is displayed.
- **Netmask** - If the Wireless AP's IP address is configured statically, the netmask that is statically configured for the Wireless AP.
- **Gateway** - If the Wireless AP's IP address is configured statically, the IP address of the gateway router that the Wireless AP will use.
- **WM Search List** - The list of IP addresses that the Wireless AP is configured to try to connect to in the event that the current connection to the Summit WM Controller is lost.

To export and save a report in XML:

1 On the report page, click **Export**. A Windows **File Download** dialog is displayed.

2 Click **Save**. A Windows **Save As** dialog is displayed.

NOTE

*If your default XML viewer is Internet Explorer or Netscape, clicking **Open** will open the exported data to your display page. You must right-click to go back to the export display. The XML data file will not be saved to your local drive.*

3 Browse to the location where you want to save the exported XML data file, and in the **File name** box enter an appropriate name for the file.

4 Click **Save**. The XML data file is saved in the specified location.

Call Detail Records (CDRs)

You can configure the Summit WM Controller to generate Call Detail Records (CDRs), which contain usage information about each wireless session per WM-AD. For more information on how to configure the Summit WM Controller to generate CDRs, refer to "Defining accounting methods for a WM-AD" on page 179.

CDRs are located in a CDR directory on the Summit WM Controller. To access the CDR file, you must first back up the file on the local drive, and then upload it to a remote server. After the CDR file is uploaded to a remote server, you can work with the file to view CDRs or import the records to a reporting tool.

You can back up and upload the file on the remote server either via the Summit WM GUI or CLI.

CDR files

CDRs are written to a file on the Summit WM Controller. The filename is based on the creation time of the CDR file with the following format: YYYYMMDDhhmmss.<ext>

- **YYYY** - Four digit year
- **MM** - Two digit month, padded with a leading zero if the month number is less than 10
- **DD** - Two digit day of the month, padded with a leading zero if the day number is less than 10
- **hh** - Two digit hour, padded with a leading zero if the hour number is less than 10
- **mm** - Two digit minute, padded with a leading zero if the minute number is less than 10
- **ss** - Two digit second, padded with a leading zero if the second number is less than 10
- **<ext>** - File extension, either .work or .dat

CDR file types

The following two types of CDR files exist in the CDR directory on the Summit WM200/2000 Controller:

- .**work** - This file is the active file that is being updated by the accounting system. The file is closed and renamed with the .dat extension when it attains its maximum size - 16 MB - or it has been open for the maximum allowed duration - 12 hours. You can back up and copy .work file from the Summit WM Controller to a remote server.
- .**dat** - This file is the inactive file that contains the archived account records. You can back up and copy the .dat file from the Summit WM Controller to a remote server.

NOTE

The CDR directory on the Summit WM Controller only has two files - a .work file and a .dat file. When the .work file attains its maximum size of 16 MB, or it has been open for 12 hours, it is saved as a .dat file. This new .dat file overwrites the existing .dat file. If you want to copy the existing .dat file, you must do so before it is overwritten by the new .dat file.

NOTE

CDRs' file format and file types in the Summit WM20 Controller are identical to the Summit WM100/1000 Controller. For more information, see the Summit WM User Guide.

The CDR directory in the Summit WM100/1000 Controller contains eight subdirectories - one directory for each day of the week and an additional working directory. You can backup and copy CDRs for the previous seven days as the new records are being created for the current day in the working directory.

Each subdirectory can contain a maximum of 48 files. The maximum size of each file is 500 MB, and the maximum time that a file can remain open is 30 minutes.

The CDR files are saved with .dat extension.

CDR file format

A CDR file contains a sequence of CDR records. The file is a standard ASCII text file. Records are separated by a sequence of dashes followed by a line break. The individual fields of a record are reported one per line, in "field=value' format.

The following table describes the records that are displayed in a CDR file.

NOTE

Most of the CDR records are typical RADIUS server attributes. For more information, refer to the user manual of your RADIUS server.

Table 28: CDR Records and their description

CDR Records	Description
Acct-Session-ID	A unique CDR ID
User-Name	The name of the user, who was authenticated.
Filter-ID	The name of the filter list for the user.
Acct-Interim-Interval	The number of seconds between interim accounting updates.
Session-Timeout	The maximum number of seconds of service to be provided to the user before termination of the session.
Class	This field is copied from the Access-Accept message sent by the RADIUS server during authentication.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Delay-Time	Indicates how many seconds the client tried to authenticate send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.

Table 28: CDR Records and their description (Continued)

CDR Records	Description
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS (AAA), Local (Internal CP) or Remote (External CP). The field displays one of the following values: 1 - AAA authentication 2 - Internal CP authentication 3 - External CP authentication
Framed-IP-Address	Indicates the address to be configured for the user
Connect-Info	This field is sent from the NAS to indicate the nature of the users' connection - 802.11b for Radio b/g or 802.11a for radio a.
NAS-Port-Type	Indicates RADIUS NAS Port Type is Altitude 802.11
Called-Station-ID	The Altitude AP's MAC address.
Calling-Station-ID	The client's MAC address.
Extreme-AP-Serial	The Altitude AP's serial number.
Extreme-AP-Name	The Altitude AP's name.
Extreme-WM-AD-Name	The WM-AD name on which the session took place.
Extreme-SSID	The SSID name on which the session took place.
Acct-Session-Time	The number of seconds the user has received the service.
Acct-Output-Packets	The number of packets that were sent to the port in the course of delivering this service to a framed user.
Acct-Input-Packets	The number of packets that have been received from the port over the course of this service being provided to a Framed User.
Acct-Output-Octets	The number of octets that were sent to the port in the course of delivering the service.
Acct-Input-Octets	The number of octets that were received from the port over the course of the service.
Acct-Terminate-Cause	Indicates how the session was terminated. The field displays one of the following values: 1 - User Request 4 - Idle Timeout 5 - Session Timeout 6 - Admin Reset 11 - NAS Reboot 16 - Callback 17 - User Error
Authenticated_time	Indicates the time at which the client was authenticated. The time is in the following format: Date hh:mm:ss. For example, April 21 2008 14:50:24
Disassociation_time	Indicates the time at which the client was disassociated from the Altitude AP. The time is in the following format: Date hh:mm:ss. For example, April 21 2008 14:57:20.

Viewing CDRs

The following is a high-level overview of how to view CDRs:

- Back up the CDR files on the local drive of the Summit WM Controller.
- Copy the CDR files from the Summit WM Controller to the remote server.
- Unzip the file.
- Download the CDR files from the remote server to view CDRs.

NOTE

You cannot access the CDR files directly from the CDR directory.

When you back up CDRs, both the .work and .dat files are zipped into a single .zip file. This .zip file is uploaded on the remote server. You can unzip this file from the remote server to extract the .work and .dat files.When you back up CDRs, the eight CDR files - one for each day of the week, and an additional working file - are zipped into a single .zip file. This .zip file is uploaded on the remote server. You can unzip this file from the remote server to extract the eight CDR files.

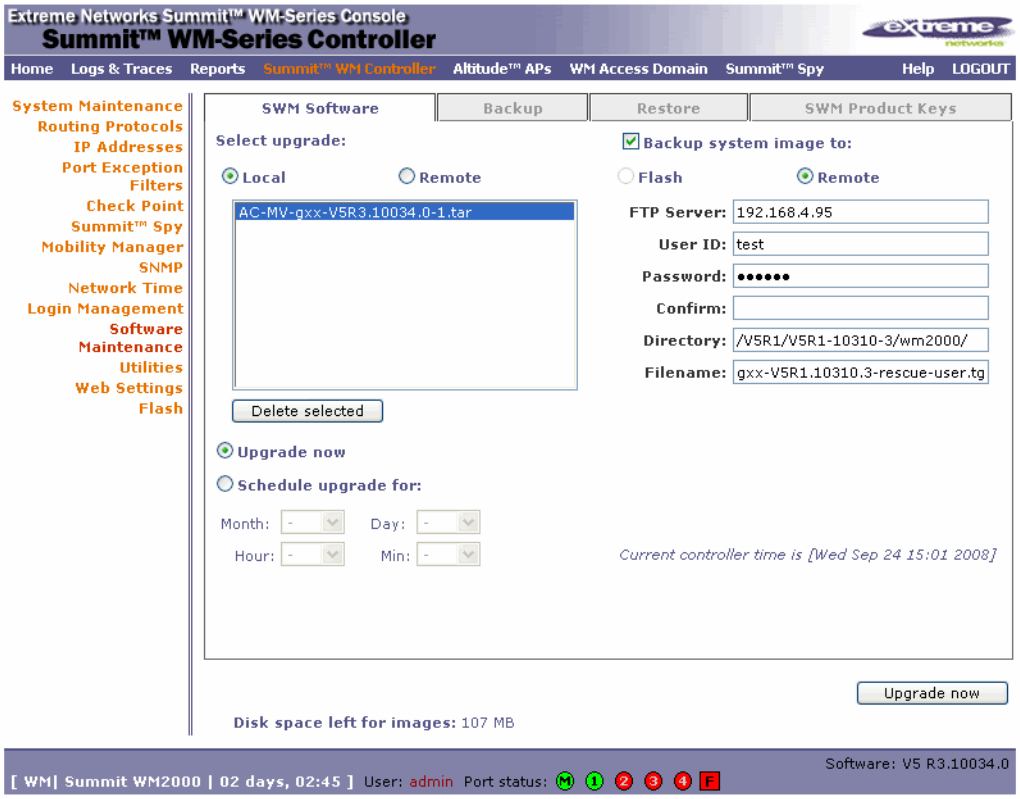
You can back up and upload the files on the remote server either via the Summit WM GUI or CLI.

This section describes how to back up and copy the CDR files to a remote server via the Summit WM GUI. For more information on how to copy the CDR file to the remote server via CLI, refer to the *Summit WM CLI Reference Guide*.

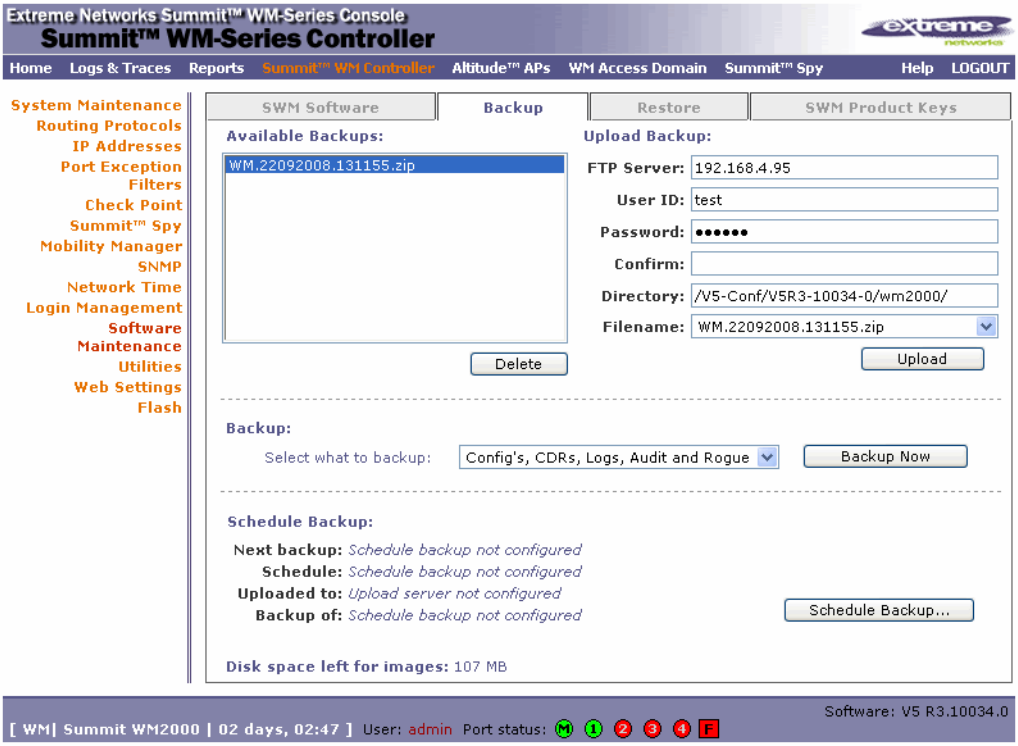
To back up and copy the CDR files to a remote server:

1 From the main menu, click **Wireless Controller Configuration**. The **Wireless Controller Configuration** page is displayed.

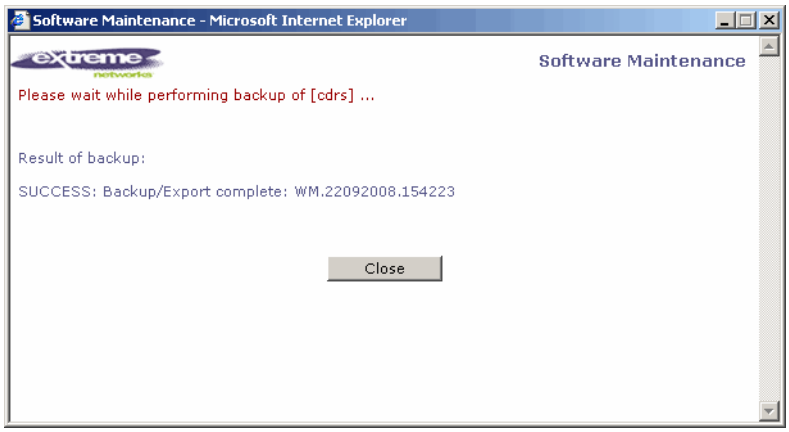
2 From the left pane, click **Software Maintenance**. The **Software Maintenance** page is displayed.



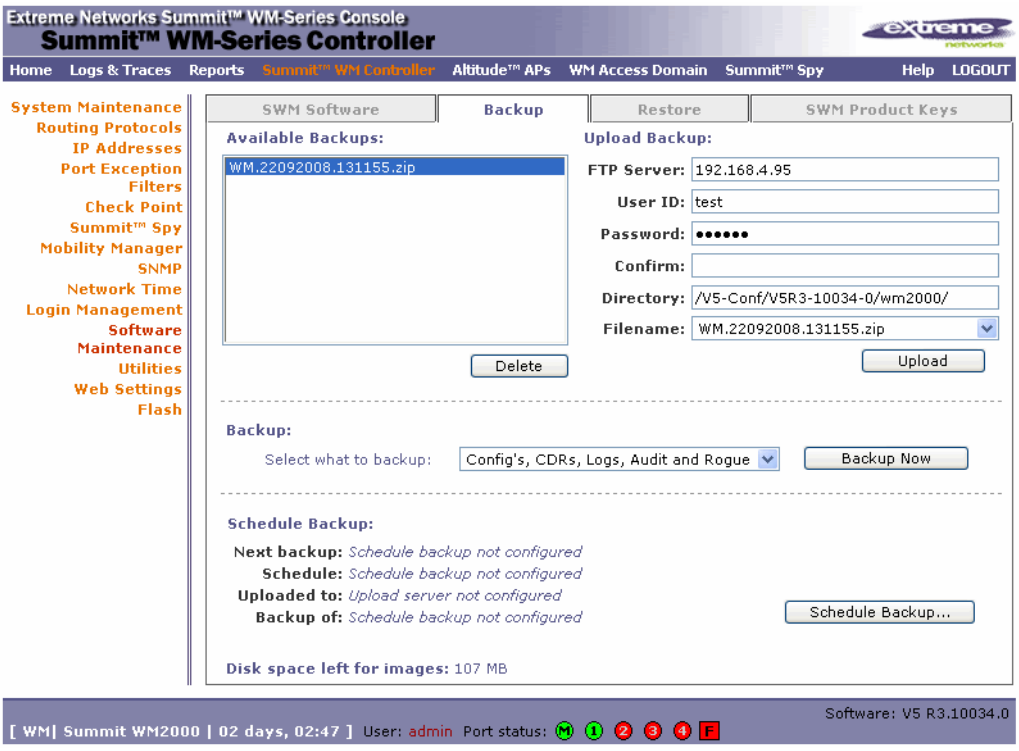
3 Click the **Backup** tab. The **Backup** page is displayed.



4 From the **Select what to backup** drop-down menu, click **CDRs only**, and then click **Backup Now**. The following window displays the backup status.


Software Maintenance - Microsoft Internet Explorer
Software Maintenance
Please wait while performing backup of [cdrs] ...
Result of backup:
SUCCESS: Backup/Export complete: WM.22092008.154223
Close

5 To close the window, click **Close**. The backed-up file is displayed in the **Available Backups** box.



NOTE

The .work and .dat files are zipped into a single file.The eight CDR files - one for each day of the week, and an additional working file - are zipped into a single .zip file.

6 In the **Upload Backup** section, type the following:

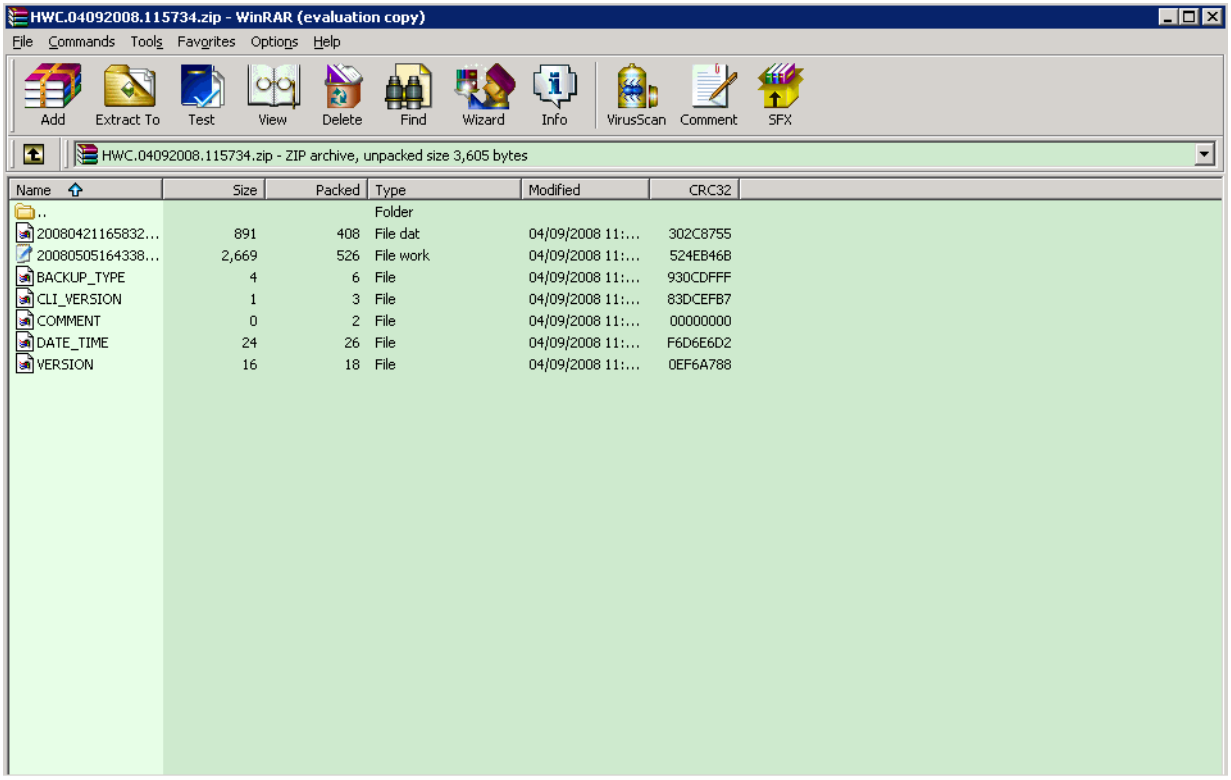
- **FTP Server** - The IP address of the FTP server.
- **User ID** - The user ID to log on the FTP server.
- **Password** - The password to log on the FTP server.
- **Confirm** - The password to confirm the password.
- **Directory** - The directory in which you want to upload the CDR file.
- **Filename** - Type the zipped CDR file name.

NOTE

After you back up CDRs, the zipped CDR file name is selected by default in the Filename box.

7 In the **Upload Backup** section, click **upload**. The .zip file is uploaded on the FTP server.

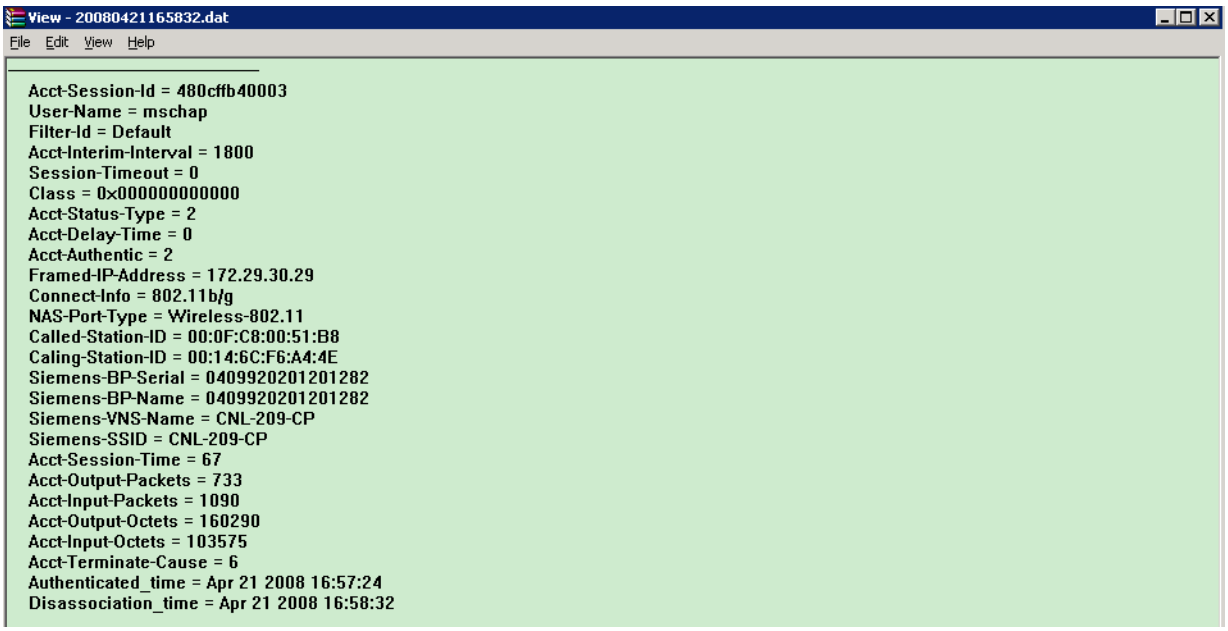
8 Unzip the file. The two CDR files - .work and .dat - are visible on the FTP server's GUI. Eight CDR files - one for each day of the week, and an additional working file - are visible on the FTP server's GUI.


HWC.04092008.115734.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
HWC.04092008.115734.zip - ZIP archive, unpacked size 3,605 bytes
Name Size Packed Type Modified CRC32
.. Folder
20080421165832... 891 408 File dat 04/09/2008 11:... 302C8755
20080505164338... 2,669 526 File work 04/09/2008 11:... 524EB46B
BACKUP_TYPE 4 6 File 04/09/2008 11:... 930CDFFF
CLI_VERSION 1 3 File 04/09/2008 11:... 83DCEFB7
COMMENT 0 2 File 04/09/2008 11:... 00000000
DATE_TIME 24 26 File 04/09/2008 11:... F6D6E6D2
VERSION 16 18 File 04/09/2008 11:... 0EF6A788

9 To view CDRs, download the files.

NOTE

The following is the screenshot of a .dat file.


View - 20080421165832.dat
File Edit View Help
Acct-Session-Id = 480cffb40003
User-Name = mschap
Filter-Id = Default
Acct-Interim-Interval = 1800
Session-Timeout = 0
Class = 0x000000000000
Acct-Status-Type = 2
Acct-Delay-Time = 0
Acct-Authentic = 2
Framed-IP-Address = 172.29.30.29
Connect-Info = 802.11b/g
NAS-Port-Type = Wireless-802.11
Called-Station-ID = 00:0F:C8:00:51:B8
Caling-Station-ID = 00:14:6C:F6:A4:4E
Siemens-BP-Serial = 0409920201201282
Siemens-BP-Name = 0409920201201282
Siemens-VNS-Name = CNL-209-CP
Siemens-SSID = CNL-209-CP
Acct-Session-Time = 67
Acct-Output-Packets = 733
Acct-Input-Packets = 1090
Acct-Output-Octets = 160290
Acct-Input-Octets = 103575
Acct-Terminate-Cause = 6
Authenticated_time = Apr 21 2008 16:57:24
Disassociation_time = Apr 21 2008 16:58:32

11 Performing system administration

This chapter describes system administration processes, including:

- "Performing Altitude AP client management" on page 297
- "Defining management users" on page 301
- "Configuring the network time" on page 303
- "Configuring Web session timeouts" on page 305

Performing Altitude AP client management

There are times when for business service or security reasons, you want to cut the connection with a particular wireless device. You can view all the associated wireless devices, by MAC address, on a selected Altitude AP and do the following:

- Disassociate a selected wireless device from its Altitude AP.
- Add a selected wireless device's MAC address to a blacklist of wireless clients that will not be allowed to associate with the Altitude AP.
- Backup and restore the Summit WM Controller database. For more information, see the *Summit WM Maintenance Guide*.

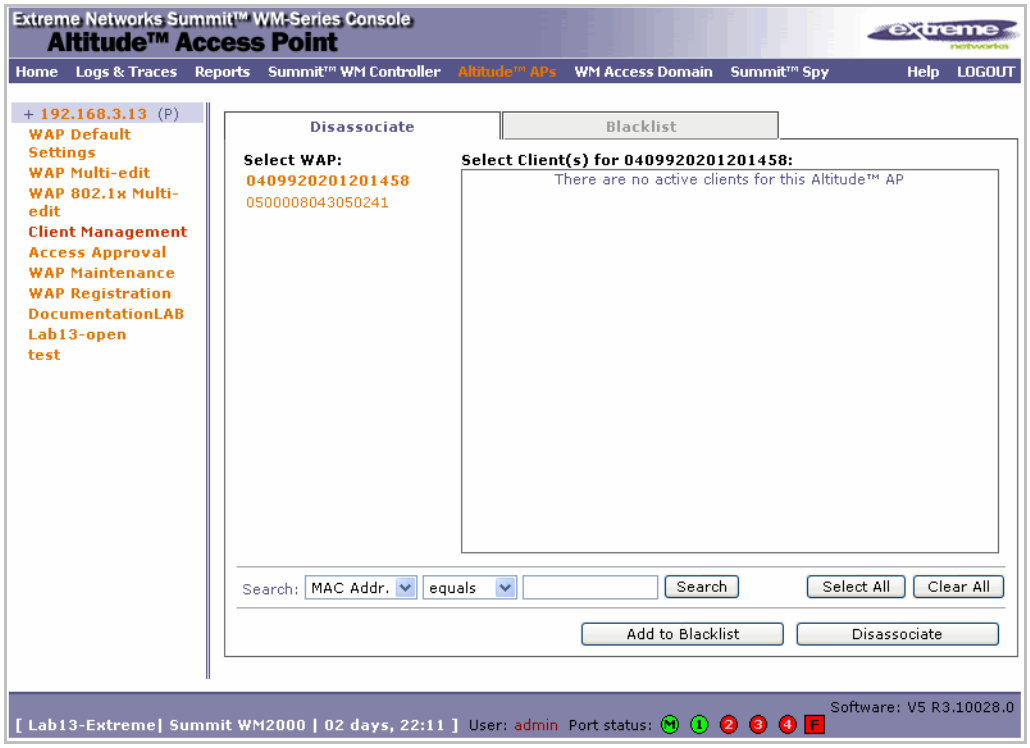
Disassociating a client

In addition to the following procedure below, you can also disassociate wireless users directly from the **Active Clients by WM-AD** page. For more information, see Chapter 10, "Working with reports and displays."

To disassociate a wireless device client:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



3 In the **Select WAP** list, click the WAP you want to disassociate.

4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate.

NOTE

*You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the **Search** box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.*

5 Click **Disassociate**. The client's session terminates immediately.

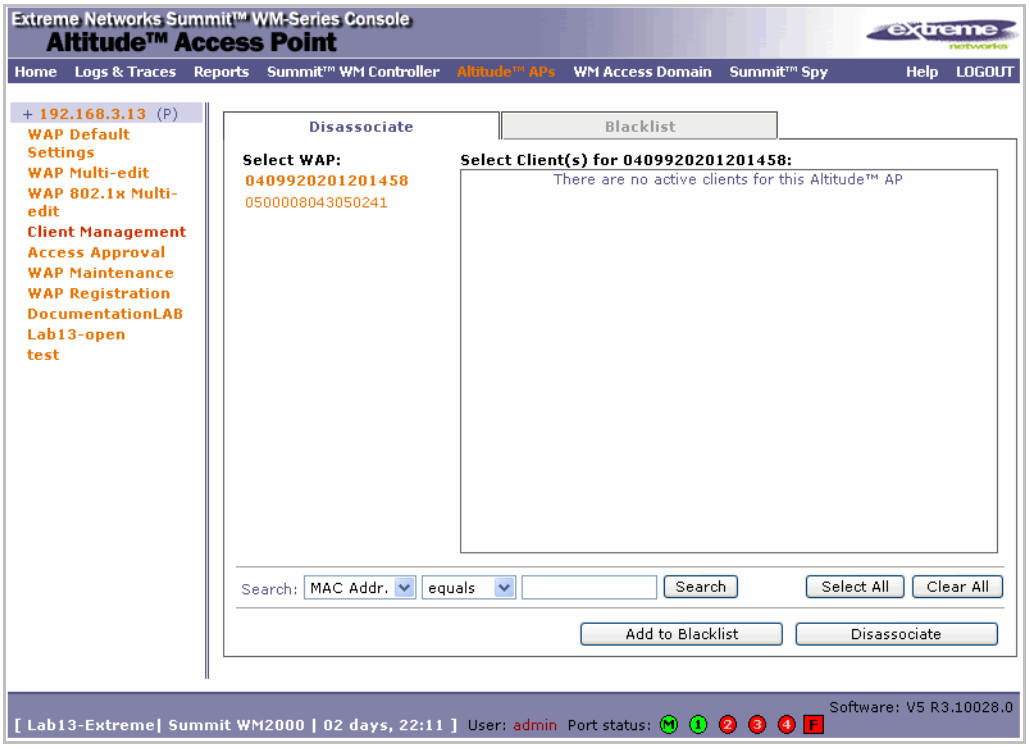
Blacklisting a client

The **Blacklist** tab displays the current list of MAC addresses that are not allowed to associate. A client is added to the blacklist by selecting it from a list of associated APs or by typing its MAC address.

To blacklist a wireless device client:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.



3 In the **Select WAP** list, click the AP you want to disassociate.

4 In the **Select Client(s)** list, select the checkbox next to the client you want to disassociate, if applicable.

NOTE

*You can search for a client by MAC Address, IP Address or User ID, by selecting the search parameters from the drop-down lists and typing a search string in the **Search** box and clicking **Search**. You can also use the **Select All** or **Clear All** buttons to help you select multiple clients.*

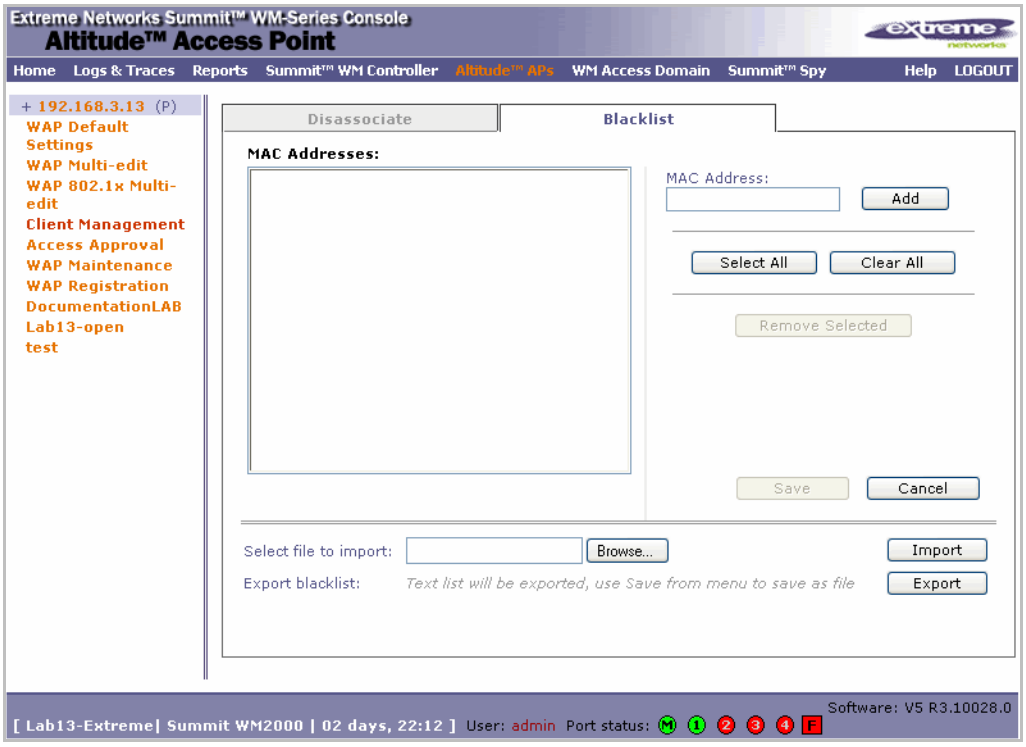
5 Click **Add to Blacklist**. The selected wireless client's MAC address is added to the blacklist.

To blacklist a wireless device client using its MAC address:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.



4 To add a new MAC address to the blacklist, in the **MAC Address** box type the client's MAC address.

5 Click **Add**. The client is displayed in the **MAC Addresses** list.

NOTE

*You can use the **Select All** or **Clear All** buttons to help you select multiple clients.*

6 To save your changes, click **Save**.

To clear an address from the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 To clear an address from the blacklist, select the corresponding checkbox in the **MAC Addresses** list.

5 Click **Remove Selected**. The selected client is removed from the list.

NOTE

*You can use the **Select All** or **Clear All** buttons to help you select multiple clients.*

6 To save your changes, click **Save**.

To import a list of MAC addresses for the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 Click **Browse** and navigate to the file of MAC addresses you want to import and add to the blacklist.

5 Click the file, and then click **Import**. The list of MAC addresses is imported.

To export a list of MAC addresses for the blacklist:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** page is displayed.

2 From the left pane, click **Client Management**. The **Disassociate** tab is displayed.

3 Click the **Blacklist** tab.

4 To export the current blacklist, use the browser's save option to save the file as a text (.txt) file. It is recommend that a descriptive file name is used.

5 Click **Export**. The saved blacklist file is exported.

Defining management users

You can define the login user names that have access to the Summit WM GUI, either for Summit WM Software administrators with read/write privileges, or users with read only privileges. For each user added, you can also define and modify a user ID and password.

When adding or modifying a management user, note the following password character constraints:

- Allowed characters include A-Z a-z 0-9 ~!@#$%^&*()_+|-=\{}[];<>?,.
- Characters not allowed include / ` ' " : and space is not valid.

To add a Summit WM Controller management user:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Login Management**. The **Login Authentication** tab is displayed.

- The **user_admin** list displays Admin users who have read/write privileges.
- The **user_read** list is for users who have read only privileges.

3 From the **Group** drop-down list, click **Admin** or **Read only**.

4 In the **User ID** box, type the user ID for the new user. A User ID can only be used once, in only one category.

5 In the **Password** box, type the password for the new user.

6 In the **Confirm Password**, retype the password.

7 Click **Add User**. The new user is added to the appropriate user list.

To modify a Summit WM management user:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Login Management**. The **Local Authentication** tab is displayed.

3 Click the **user** you want to modify.

4 In the **Password** box, type the new password for the user.

5 In the **Confirm Password**, retype the new password.

6 To change the Password, click **Change Password**.

To remove a Summit WM Controller management user:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Login Management**. The **Local Authentication** tab is displayed.

3 Click the user you want to remove.

4 To remove the user, click **Remove user**. The user is removed from the list.

Configuring the network time

The internal clocks of the Summit WM Controller and Altitude APs on a network may differ. You should synchronize the clocks of the Summit WM Controller and the Altitude APs to ensure that the logs and reports reflect accurate time stamps. For more information, see Chapter 10, "Working with reports and displays".

NOTE

The normal operation of the Summit WM Controller will not be affected if you do not synchronize the clock. The clock synchronization is necessary to ensure that the logs bear the accurate time stamps. In addition, the clock synchronization of network elements is a pre-requisite for the following configurations:

- Mobility Manager
- Session Availability

The Summit WM Controller provides the following two options to synchronize the clocks of the Summit WM Controller and the Altitude APs:

- Using the system's time - The system's time is the Summit WM Controller's time.
- Using the network time protocol (NTP) - The Network Time Protocol is a protocol for synchronizing the clocks of computer systems over packet-switched data networks.

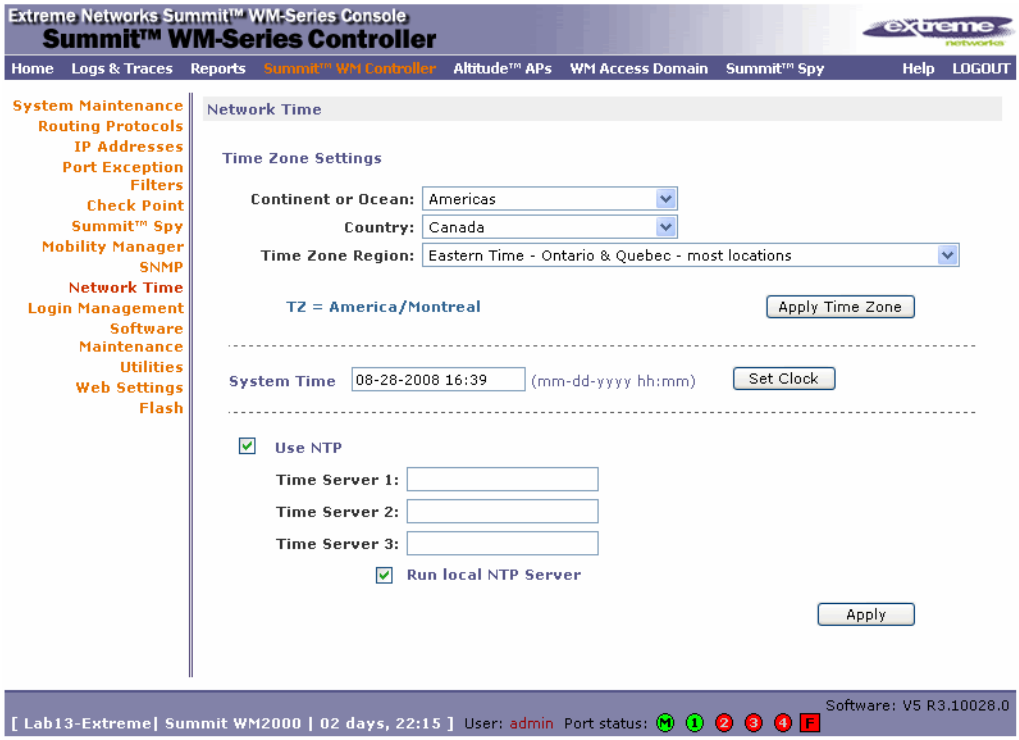
Configuring the network time using the system's time

To configure the network time, using the system's time:

1 Login on the Summit WM Controller. The **Summit WM GUI** is displayed.

2 Click **Wireless Controller Configuration**. The **Wireless Controller Configuration** screen is displayed.

3 In the left pane, click **Network Time**. The **Network Time** screen is displayed.



4 From the **Continent or Ocean** drop-down list, click the appropriate large-scale geographic grouping for the time zone.

5 From the **Country** drop-down list, click the appropriate country for the time zone. The contents of the drop-down list change, based on the selection in the **Continent or Ocean** drop-down list.

6 From the **Time Zone Region** drop-down list, click the appropriate time zone region for the selected country.

7 Click **Apply Time Zone**.

NOTE

Changing the Time Zone causes the Summit WM Controller to reboot.

8 Select the **Use System Time** radio button.

You can modify the system's date and time by changing the entries in the **Use System Time** text box. The date is in **mm-dd-yyyy** format and the time is in hh:mm format.

9 Click **Apply**.

10 Reboot the Summit WM Controller. The WLAN network time is synchronized in accordance with the Summit WM Controller's time.

Configuring the network time using the NTP

To configure the network time using the NTP:

1 Perform Steps 1 to 7 of "Configuring the network time using the system's time" on page 303.

2 Select **Use NTP** radio button.

NOTE

If you want to use the Summit WM Controller as the NTP Server, select the Run local NTP Server checkbox, and then skip to Step 5.

3 In the **Time Server 1** text box, type the IP address or FQDN (Full Qualified Domain Name) of a NTP Time Server that is accessible on the enterprise network.

4 Repeat Step 3 for **Time Server 2** and **Time Server 3** text boxes.

If the system is not able to connect to the **Time Server 1**, it will attempt to connect to the additional servers that have been specified in **Time Server 2** and **Time Server 3** text boxes.

5 From the left pane, click **Software Maintenance**. The **System Maintenance** page is displayed.

6 Click the **Apply**.

7 Reboot the Summit WM Controller. The WLAN network time is synchronized in accordance with the specified time server.

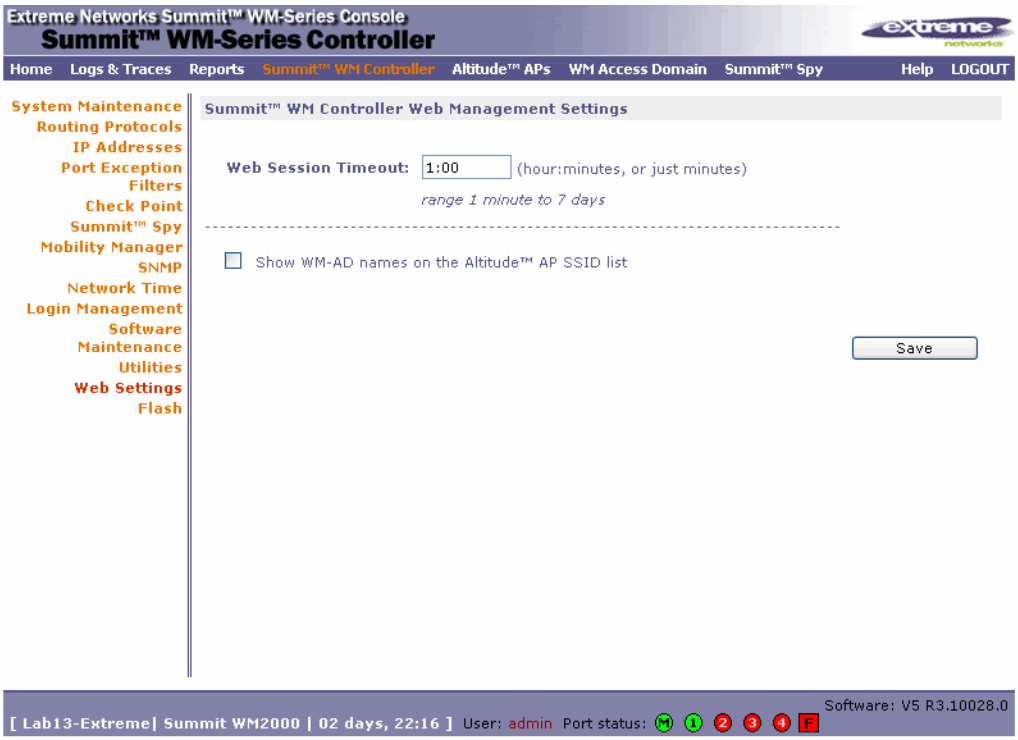
Configuring Web session timeouts

You can configure the time period to allow Web sessions to remain inactive before timing out.

To configure Web session timeouts:

1 From the main menu, click **Summit Controller Configuration**. The **Summit Controller Configuration** page is displayed.

2 In the left pane, click **Web Settings**. The **Summit WM Controller Web Management Settings** page is displayed.



3 In the **Web Session Timeout** box, type the time period to allow the Web session to remain inactive before it times out. This can be entered as hour:minutes, or as minutes. The range is 1 minute to 168 hours.

4 Select the **Show WM-AD names on the Altitude AP SSID list** checkbox to allow the names of the WM-ADs to appear in the SSID list for Altitude APs.

5 To save your settings, click **Save**.

NOTE

Pages that auto-refresh will time-out unless a manual action takes place prior to the end of the timeout period.

Glossary

Networking terms and abbreviations

Term	Explanation
AAA	Authentication, Authorization and Accounting. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.
Access Point (AP)	A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices.
Ad-hoc mode	An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). (Compare Infrastructure Mode)
AES	Advanced Encryption Standard (AES) is an algorithm for encryption that works at multiple network layers simultaneously. As a block cipher, AES encrypts data in fixed-size blocks of 128 bits. AES was created by the National Institute of Standards and Technology (NIST). AES is a privacy transform for IPSec and Internet Key Exchange (IKE). AES has a variable key length - the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key. For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.
AES-CCMP	AES uses the Counter-Mode/CBC-MAC Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The two underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.
ARP	Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.
Association	A connection between a wireless device and an Access Point.
asynchronous	Asynchronous transmission mode (ATM). A start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

Term	Explanation
BSS	Basic Service Set. A wireless topology consisting of one Access Point connected to a wired network and a set of wireless devices. Also called an infrastructure network. *See also* IBSS.
Captive Portal	A browser-based authentication mechanism that forces unauthenticated users to a Web page. Sometimes called a "reverse firewall".
CDR	Call Data (Detail) Record In Internet telephony, a call detail record is a data record that contains information related to a telephone call, such as the origination and destination addresses of the call, the time the call started and ended, the duration of the call, the time of day the call was made and any toll charges that were added through the network or charges for operator services, among other details of the call. In essence, call accounting is a database application that processes call data from your switch (PBX, iPBX, or key system) via a CDR (call detail record) or SMDR (station message detail record) port. The call data record details your system's incoming and outgoing calls by thresholds, including time of call, duration of call, dialing extension, and number dialed. Call data is stored in a PC database
CHAP	Challenge-Handshake Authentication Protocol. One of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.
CLI	Command Line Interface.
Collision	Two Ethernet packets attempting to use the medium simultaneously. Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. When two nodes at different locations attempt to send data at the same time, a collision will result. Segmenting the network with bridges or switches is one way of reducing collisions in an overcrowded network.
Datagram	A datagram is "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." (RFC1594). The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports.
Decapsulation	*See* tunnelling.
Device Server	A specialized, network-based hardware device designed to perform a single or specialized set of server functions. Print servers, terminal servers, remote access servers and network time servers are examples of device servers.

Term	Explanation
DHCP	Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. (IETF RFC1531.) Option 78 specifies the location of one or more SLP Directory Agents. Option 79 specifies the list of scopes that a SLP Agent is configured to use.(RFC2610 - DHCP Options for Service Location Protocol)
Directory Agent (DA)	A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request. For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent. (SLP version 2, RFC2608, updating RFC2165)
Diversity antenna and receiver	The AP has two antennae. Receive diversity refers to the ability of the AP to provide better service to a device by receiving from the user on which ever of the two antennae is receiving the cleanest signal. Transmit diversity refers to the ability of the AP to use its two antenna to transmit on a specific antenna only, or on a alternate antennae. The antennae are called diversity antennae because of this capability of the pair.
DNS	Domain Name Server
DSSS	Direct-Sequence Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare FHSS)
DTIM	DTIM delivery traffic indication message (in 802.11 standard)

Term	Explanation
Dynamic WEP	The IEEE introduced the concept of user-based authentication using per-user encryption keys to solve the scalability issues that surrounded static WEP. This resulted in the 802.1X standard, which makes use of the IETF's Extensible Authentication Protocol (EAP), which was originally designed for user authentication in dial-up networks. The 802.1X standard supplemented the EAP protocol with a mechanism to send an encryption key to a Wireless AP. These encryption keys are used as dynamic WEP keys, allowing traffic to each individual user to be encrypted using a separate key.
EAP-TLS **EAP-TTLS**	EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1X specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication. EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys. EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates. (*See also* PEAP)
ELA (OPSEC)	Event Logging API (Application Program Interface) for OPSEC, a module in Check Point used to enable third-party applications to log events into the Check Point VPN-1/FireWall-1 management system.
Encapsulation	*See* tunnelling.
ESS	Extended Service Set (ESS). Several Basic Service Sets (BSSs) can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. (*See* BSS and SSID.)
FHSS	Frequency-Hopping Spread Spectrum. A transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare DSSS)

Term	Explanation
Fit, thin and fat APs	A thin AP architecture uses two components: an access point that is essentially a stripped-down radio and a centralized management controller that handles the other WLAN system functions. Wired network switches are also required. A fit AP, a variation of the thin AP, handles the RF and encryption, while the central management controller, aware of the wireless users' identities and locations, handles secure roaming, quality of service, and user authentication. The central management controller also handles AP configuration and management. A fat (or thick) AP architecture concentrates all the WLAN intelligence in the access point. The AP handles the radio frequency (RF) communication, as well as authenticating users, encrypting communications, secure roaming, WLAN management, and in some cases, network routing.
FQDN	Fully Qualified Domain Name. A "friendly" designation of a computer, of the general form computer.[subnetwork.].organization.domain. The FQDN names must be translated into an IP address in order for the resource to be found on a network, usually performed by a Domain Name Server.
FTM	Forwarding Table Manager
FTP	File Transfer Protocol
Gateway	In the wireless world, an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.
Gigabit Ethernet	The high data rate of the Ethernet standard, supporting data rates of 1 gigabit (1,000 megabits) per second.
GUI	Graphical User Interface
Heartbeat message	A heartbeat message is a UDP data packet used to monitor a data connection, polling to see if the connection is still alive. In general terms, a heartbeat is a signal emitted at regular intervals by software to demonstrate that it is still alive. In networking, a heartbeat is the signal emitted by a Level 2 Ethernet transceiver at the end of every packet to show that the collision-detection circuit is still connected.
Host	(1) A computer (usually containing data) that is accessed by a user working on a remote terminal, connected by modems and telephone lines. (2) A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.
HTTP	Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. A Web browser makes use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)

Term	Explanation
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL, is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS uses Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.
IBSS	Independent Basic Service Set. *See* BSS. An IBSS is the 802.11 term for an adhoc network. *See* adhoc network.
ICMP	Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC792. ICMP supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.
ICV	ICV (Integrity Check Value) is a 4-byte code appended in standard WEP to the 802.11 message. Enhanced WPA inserts an 8-byte MIC just before the ICV. (*See* WPA and MIC)
IE	Internet Explorer.
IEEE	Institute of Electrical and Electronics Engineers, a technical professional association, involved in standards activities.
IETF	Internet Engineering Task Force, the main standards organization for the Internet.
Infrastructure Mode	An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. (*See* ad-hoc mode and BSS.)
Internet or IP telephony	IP or Internet telephony are communications, such as voice, facsimile, voice-messaging applications, that are transported over the Internet, rather than the public switched telephone network (PSTN). IP telephony is the two-way transmission of audio over a packet-switched IP network (TCP/IP network). An Internet telephone call has two steps: (1) converting the analog voice signal to digital format, (2) translating the signal into Internet protocol (IP) packets for transmission over the Internet. At the receiving end, the steps are reversed. Over the public Internet, voice quality varies considerably. Protocols that support Quality of Service (QoS) are being implemented to improve this.
IP	Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (host) on the Internet has at least one IP address that uniquely identifies it. Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

Term	Explanation
IPC	Interprocess Communication. A capability supported by some operating systems that allows one process to communicate with another process. The processes can be running on the same computer or on different computers connected through a network.
IPsec	Internet Protocol security (IPSec)
IPsec-ESP **IPsec-AH**	Internet Protocol security Encapsulating Security Payload (IPsec-ESP). The encapsulating security payload (ESP) encapsulates its data, enabling it to protect data that follows in the datagram.Internet Protocol security Authentication Header (IPsec-AH). AH protects the parts of the IP datagram that can be predicted by the sender as it will be received by the receiver.IPsec is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet. For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the receiver to obtain a public key and authenticate the sender using digital certificates.
isochronous	Isochronous data is data (such as voice or video) that requires a constant transmission rate, where data must be delivered within certain time constraints. For example, multimedia streams require an isochronous transport mechanism to ensure that data is delivered as fast as it is displayed and to ensure that the audio is synchronized with the video. Compare: asynchronous processes in which data streams can be broken by random intervals, and synchronous processes, in which data streams can be delivered only at specific intervals.
ISP	Internet Service Provider.
IV	IV (Initialization Vector), part of the standard WEP encryption mechanism that concatenates a shared secret key with a randomly generated 24-bit initialization vector. WPA with TKIP uses 48-bit IVs, an enhancement that significantly increases the difficulty in cracking the encryption. (*See* WPA and TKIP)
LAN	Local Area Network.
License installation	
LSA	Link State Advertisements received by the currently running OSPF process. The LSAs describe the local state of a router or network, including the state of the router's interfaces and adjacencies. *See* also OSPF.
MAC	Media Access Control layer. One of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

Term	Explanation
MAC address	Media Access Control address. A hardware address that uniquely identifies each node of a network.
MIB	Management Information Base is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP. A MIB is a collection of definitions defining the properties of a managed object within a device. Every managed device keeps a database of values for each of the definitions written in the MIB. Definition of the MIB conforms to RFC1155 (Structure of Management Information).
MIC	Message Integrity Check or Code (MIC), also called "Michael", is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte integrity check value (ICV) that is appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks. Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with. (*See* WPA, TKIP and ICV).
MTU	Maximum Transmission Unit. The largest packet size, measured in bytes, that a network interface is configured to accept. Any messages larger than the MTU are divided into smaller packets before being sent.
MU	Mobile Unit, a wireless device such as a PC laptop.
multicast, broadcast, unicast	Multicast: transmitting a single message to a select group of recipients. Broadcast: sending a message to everyone connected to a network. Unicast: communication over a network between a single sender and a single receiver.
NAS	Network Access Server, a server responsible for passing information to designated RADIUS servers and then acting on the response returned. A NAS-Identifier is a RADIUS attribute identifying the NAS server. (RFC2138)
NAT	Network Address Translator. A network capability that enables a group of computers to dynamically share a single incoming IP address. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.
Netmask	In administering Internet sites, a netmask is a string of 0's and 1's that mask or screen out the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the "255.255.255.0" netmask allows the specific host computer address to be visible.
NIC	Network Interface Card. An expansion board in a computer that connects the computer to a network.
NMS	Network Management System. The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, which reside in the managed nodes.

Term	Explanation
NTP	Network Time Protocol, an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Based on UTC, NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock. (RFC1305)
OFDM	Orthogonal frequency division multiplexing, a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. OFDM is similar to conventional frequency division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels. OFDM is used in European digital audio broadcast services. It is also used in wireless local area networks.
OID	Object Identifier.
OPSEC	OPSEC (Open Platform for Security) is a security alliance program created by Check Point to enable an open industry-wide framework for interoperability of security products and applications. Products carrying the "Secured by Check Point" seal have been tested to guarantee integration and interoperability.
OS	Operating system.
OSI	Open System Interconnection. An ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, down through the presentation, session, transport, network, data link layer to the physical layer at the bottom, over the channel to the next station and back up the hierarchy.
OSI Layer 2	At the Data Link layer (OSI Layer 2), data packets are encoded and decoded into bits. The data link layer has two sublayers: • The Logical Link Control (LLC) layer controls frame synchronization, flow control and error checking • The Media Access Control (MAC) layer controls how a computer on the network gains access to the data and permission to transmit it.
OSI Layer 3	The Network layer (OSI Layer 3) provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Term	Explanation
OSPF	Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. The host using OSPF sends only the part that has changed, and only when a change has taken place. (RFC2328)
OUI	Organizationally Unique Identifier (used in MAC addressing).
Packet	The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into packets. Each packet is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).
PAP	Password Authentication Protocol is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. (*See* CHAP).
PDU	Protocol Data Unit. A data object exchanged by protocol machines (such as management stations, SMUX peers, and SNMP agents) and consisting of both protocol control information and user data. PDU is sometimes used as a synonym for "packet".
PEAP	PEAP (Protected Extensible Authentication Protocol) is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (*See* also EAP-TLS).
PHP server	Hypertext Preprocessor
PKI	Public Key Infrastructure
PoE	Power over Ethernet. The Power over Ethernet standard (802.3af) defines how power can be provided to network devices over existing Ethernet connection, eliminating the need for additional external power supplies.
POST	Power On Self Test, a diagnostic testing sequence performed by a computer to determine if its hardware elements are present and powered on. If so, the computer begins its boot sequence.

Term	Explanation
push-to-talk (PTT)	The push-to-talk (PTT) is feature on wireless telephones that allows them to operate like a walkie-talkie in a group, instead of standard telephone operation. The PTT feature requires that the network be configured to allow multicast traffic. A PTT call is initiated by selecting a channel and pressing the "talk" key on the wireless telephone. All wireless telephones on the same network that are monitoring the channel will hear the transmission. On a PTT call you hold the button to talk and release it to listen.
QoS	Quality of Service. A term for a number of techniques that intelligently match the needs of specific applications to the network resources available, using such technologies as Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks. QoS features provide better network service by supporting dedicated bandwidth, improving loss characteristics, avoiding and managing network congestion, shaping network traffic, setting traffic priorities across the network. Quality-of-Service (QoS): A set of service requirements to be met by the network while transporting a flow. (RFC2386)
RADIUS	Remote Authentication Dial-In User Service. An authentication and accounting system that checks User Name and Password and authorizes access to a network. The RADIUS specification is maintained by a working group of the IETF (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).
RF	Radio Frequency, a frequency in the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that can propagate through space. These frequencies in the electromagnetic spectrum range from Ultra-low frequency (ULF) -- 0-3 Hz to Extremely high frequency (EHF) -- 30GHz - 300 GHz. The middle ranges are: Low frequency (LF) -- 30 kHz - 300 kHz, Medium frequency (MF) -- 300 kHz - 3 MHz, High frequency (HF) -- 3MHz - 30 MHz, Very high frequency (VHF) -- 30 MHz - 300 MHz, Ultra-high frequency (UHF)-- 300MHz - 3 GHz.
RFC	Request for Comments, a series of notes about the Internet, submitted to the Internet Engineering Task Force (IETF) and designated by an RFC number, that may evolve into an Internet standard. The RFCs are catalogued and maintained on the IETF RFC website: www.ietf.org/rfc.html.
Roaming	In 802.11, roaming occurs when a wireless device (a station) moves from one Access Point to another (or BSS to another) in the same Extended Service Set (ESS) -identified by its SSID.
RP-SMA	Reverse Polarity-Subminiature version A, a type of connector used with wireless antennas
RSN	Robust Security Network. A new standard within IEEE 802.11 to provide security and privacy mechanisms. The RSN (and related TSN) both specify IEEE 802.1X authentication with Extensible Authentication Protocol (EAP).
RSSI	RSSI received signal strength indication (in 802.11 standard)

Term	Explanation
RTS / CTS	RTS request to send, CTS clear to send (in 802.11 standard)
Segment	In Ethernet networks, a section of a network that is bounded by bridges, routers or switches. Dividing a LAN segment into multiple smaller segments is one of the most common ways of increasing available bandwidth on the LAN.
SLP	Service Location Protocol. A method of organizing and locating the resources (such as printers, disk drives, databases, e-mail directories, and schedulers) in a network. Using SLP, networking applications can discover the existence, location and configuration of networked devices. With Service Location Protocol, client applications are 'User Agents' and services are advertised by 'Service Agents'. The User Agent issues a multicast 'Service Request' (SrvRqst) on behalf of the client application, specifying the services required. The User Agent will receive a Service Reply (SrvRply) specifying the location of all services in the network which satisfy the request. For larger networks, a third entity, called a 'Directory Agent', receives registrations from all available Service Agents. A User Agent sends a unicast request for services to a Directory Agent (if there is one) rather than to a Service Agent. (SLP version 2, RFC2608, updating RFC2165)
SMI	Structure of Management Information. A hierarchical tree structure for information that underlies Management Information Bases (MIBs), and is used by the SNMP protocol. Defined in RFC1155 and RFC1442 (SNMPv2).
SMT (802.11)	Station ManagemenT. The object class in the 802.11 MIB that provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network. The four branches of the 802.11 MIB are: • dot11smt - objects related to station management and local configuration • dot11mac - objects that report/configure on the status of various MAC parameters • dot11res - Objects that describe available resources • dot11phy - Objects that report on various physical items.
SNMP	Simple Network Management Protocol. A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set.
SNMP trap	An event notification sent by the SNMP managed agent to the management system to identify the occurrence of conditions (such as a threshold that exceeds a predetermined value).

Term	Explanation
SSH	Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. SSH is a suite of three utilities - slogin, ssh, and scp - secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. With SSH commands, both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
SSID	Service Set Identifier. A 32-character unique identifier attached to the header of packets sent over a Wireless LAN that acts as a password when a wireless device tries to connect to the Basic Service Set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS). The SSID is used to identify the ESS. In 802.11 networks, each Access Point advertises its presence several times per second by broadcasting beacon frames that carry the ESS name (SSID). Stations discover APs by listening for beacons, or by sending probe frames to search for an AP with a desired SSID. When the station locates an appropriately-named Access Point, it sends an associate request frame containing the desired SSID. The AP replies with an associate response frame, also containing the SSID. Some APs can be configured to send a zero-length broadcast SSID in beacon frames instead of sending their actual SSID. The AP must return its actual SSID in the probe response.
SSL	Secure Sockets Layer. A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. URLs that require an SSL connection start with https: instead of http. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.
Subnet mask	(*See* netmask)
Subnets	Portions of networks that share the same common address format. A subnet in a TCP/IP network uses the same first three sets of numbers (such as 198.63.45.xxx), leaving the fourth set to identify devices on the subnet. A subnet can be used to increase the bandwidth on the network by breaking the network up into segments.
SVP	SpectraLink Voice Protocol, a protocol developed by SpectraLink to be implemented on access points in order to facilitate voice prioritization over an 802.11 wireless LAN that will carry voice packets from SpectraLink wireless telephones.

Term	Explanation
Switch	In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.
syslog	A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them. Syslog uses the user datagram protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC3164)
TCP / IP	Transmission Control Protocol. TCP, together with IP (Internet Protocol), is the basic communication language or protocol of the Internet. Transmission Control Protocol manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. Internet Protocol handles the address part of each packet so that it gets to the right destination. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.
TFTP	Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). TFTP is described formally in Request for Comments (RFC) 1350.
TKIP	Temporal Key Integrity Protocol (TKIP) is an enhancement to the WEP encryption technique that uses a set of algorithms that rotates the session keys. TKIPs' enhanced encryption includes a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. The encryption keys are changed (rekeyed) automatically and authenticated between devices after the rekey interval (either a specified period of time, or after a specified number of packets has been transmitted).
TLS	Transport Layer Security. (*See* EAP, Extensible Authentication Protocol)
ToS / DSCP	ToS (Type of Service) / DSCP (Diffserv Codepoint). The ToS/DSCP box contained in the IP header of a frame is used by applications to indicate the priority and Quality of Service (QoS) for each frame. The level of service is determined by a set of service parameters which provide a three way trade-off between low-delay, high-reliability, and high-throughput. The use of service parameters may increase the cost of service.

Term	Explanation
TSN	Transition Security Network. A subset of Robust Security Network (RSN), which provides an enhanced security solution for legacy hardware. The Wi-Fi Alliance has adopted a solution called Wireless Protected Access (WPA), based on TSN. RSN and TSN both specify IEEE 802.1X authentication with Extensible Authentication Protocol (EAP).
Tunnelling	Tunnelling (or encapsulation) is a technology that enables one network to send its data via another network's connections. Tunnelling works by encapsulating packets of a network protocol within packets carried by the second network. The receiving device then decapsulates the packets and forwards them in their original format.
UDP	User Datagram Protocol. A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive packets over an IP network. It is used primarily for broadcasting messages over a network.
U-NII	Unlicensed National Information Infrastructure. Designated to provide short-range, high-speed wireless networking communication at low cost, U-NII consists of three frequency bands of 100 MHz each in the 5 GHz band: 5.15-5.25GHz (for indoor use only), 5.25-5.35 GHz and 5.725-5.825GHz. The three frequency bands were set aside by the FCC in 1997 initially to help schools connect to the Internet without the need for hard wiring. U-NII devices do not require licensing.
URL	Uniform Resource Locator. the unique global address of resources or files on the World Wide Web. The URL contains the name of the protocol to be used to access the file resource, the IP address or the domain name of the computer where the resource is located, and a pathname -- a hierarchical description that specifies the location of a file in that computer.
VLAN	Virtual Local Area Network. A network of computers that behave as if they are connected to the same wire when they may be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. When a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration. The standard is defined in IEEE 802.1Q - Virtual LANs, which states that "IEEE 802 Local Area Networks (LANs) of all types may be connected together with Media Access Control (MAC) Bridges, as specified in ISO/IEC 15802-3. This standard defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure."
VoIP	Voice Over Internet Protocol. An internet telephony technique. With VoIP, a voice transmission is cut into multiple packets, takes the most efficient path along the Internet and is reassembled when it reaches the destination.
VPN	Virtual Private Network. A private network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Term	Explanation
VSA	Vendor Specific Attribute, an attribute for a RADIUS server defined by the manufacturer.(compared to the RADIUS attributes defined in the original RADIUS protocol RFC2865). A VSA attribute is defined in order that it can be returned from the RADIUS server in the Access Granted packet to the Radius Client.
Walled Garden	A restricted subset of network content that wireless devices can access.
WEP	Wired Equivalent Privacy. A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
Wi-Fi	Wireless fidelity. A term referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. Used in reference to the Wi-Fi Alliance, a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.
WINS	Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer, called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS supports dynamic addressing (DHCP) by maintaining a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
WLAN	Wireless Local Area Network.
WM-AD	WM Access Domain Services (WM-AD). A Extreme Networks specific technique that provides a means of mapping wireless networks to a wired topology.
WMM	Wi-Fi Multimedia (WMM), a Wi-Fi Alliance certified standard that provides multimedia enhancements for Wi-Fi networks that improve the user experience for audio, video, and voice applications. This standard is compliant with the IEEE 802.11e Quality of Service (QoS) extensions for 802.11 networks. WMM provides prioritized media access by shortening the time between transmitting packets for higher priority traffic. WMM is based on the Enhanced Distributed Channel Access (EDCA) method.
WPA	Wireless Protected Access, or Wi-Fi Protected Access is a security solution adopted by the Wi-Fi Alliance that adds authentication to WEPs' basic encryption. For authentication, WPA specifies IEEE 802.1X authentication with Extensible Authentication Protocol (EAP). For encryption, WPA uses the Temporal Key Integrity Protocol (TKIP) mechanism, which shares a starting key between devices, and then changes their encryption key for every packet. Certificate Authentication (CA) can also be used. Also part of the encryption mechanism are 802.1X for dynamic key distribution and Message Integrity Check (MIC) a.k.a. Michael. WPA requires that all computers and devices have WPA software.

Term	Explanation
WPA-PSK	Wi-Fi Protected Access with Pre-Shared Key, a special mode of WPA for users without an enterprise authentication server. Instead, for authentication, a Pre-Shared Key is used. The PSK is a shared secret (passphrase) that must be entered in both the Wireless AP or router and the WPA clients. This preshared key should be a random sequence of characters at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. After the initial shared secret, the Temporal Key Integrity Protocol (TKIP) handles the encryption and automatic rekeying.

Controller, Access Points, and WM software terms and abbreviations

Term	Explanation
CTP	CAPWAP Tunnelling Protocol (CTP). The Wireless AP uses a UDP (User Datagram Protocol) based tunnelling protocol called CAPWAP Tunnelling Protocol (CTP) to encapsulate the 802.11 packets and forward them to the Summit WM Controller. The CTP protocol defines a mechanism for the control and provisioning of Wireless APs (CAPWAP) through centralized access controllers. In addition, it provides a mechanism providing the option to tunnel the mobile client data between the access point and the access controller.
Data Collector	The Data Collector is an application on the Summit WM Controller that receives and manages the Radio Frequency (RF) scan messages sent by the Wireless AP. This application is part of the Summit WM series Spy technique, working in conjunction with the scanner mechanism and the Analysis Engine to assist in detecting rogue access points.
DRM (dynamic radio/RF management)	Dynamic Radio Management (DRM) functionality of the Summit WM Controller is used to help establish the optimum radio configuration for your Altitude APs. DRM is enabled by default. The Summit WM Controller's DRM: • Adjusts power levels to balance coverage if another Altitude AP, which is assigned to the same SSID and is on the same channel, is added to or leaves the network. • Allows wireless clients to be moved to another Altitude AP if the load is too high. • Scans automatically for a channel, using a channel selection algorithm. • Avoids other WLANs by reducing transmit power whenever other Altitude APs with the same channel, but different SSIDs are detected. The DRM feature is comprised of two functions: • Auto Channel Selection (ACS) - ACS provides an easy way to optimize channel arrangement based on the current situation in the field. ACS provides an optimal solution only if it is triggered on all Altitude APs in a deployment. Triggering ACS on a single Altitude AP or on a subset of Altitude APs provides a useful but suboptimal solution. Also, ACS only relies on the information observed at the time it is triggered. Once an Altitude AP has selected a channel, it will remain operating on that channel until the user changes the channel or triggers ACS. • Auto Tx Power Control (ATPC) - ATPC guarantees your LAN a stable RF environment by automatically adapting transmission power signals according to the coverage provided by the Altitude APs. ATPC can be either enabled or disabled.
Langley	Langley is a Controller, Access Points, and WM software term for the inter-process messaging infrastructure on the Summit WM Controller.

Term	Explanation
Mobility manager (and mobility agent)	The technique in Controller, Access Points, and WM software by which multiple Summit WM Controllers on a network can discover each other and exchange information about a client session. This enables a wireless device user to roam seamlessly between different Wireless APs on different Summit WM Controllers, to provide mobility to the wireless device user. One Summit WM Controller on the network must be designated as the mobility manager. All other Summit WM Controllers are designated as mobility agents. Relying on SLP, the mobility manager registers with the Directory Agent and the mobility agents discover the location of the mobility manager.
Summit WM Controller	The Summit WM Controller is a rack-mountable network device designed to be integrated into an existing wired Local Area Network (LAN). It provides centralized control over all access points (both Wireless APs and third-party access points) and manages the network assignment of wireless device clients associating through access points.
Summit WM series Spy	The Summit WM series Spy is a mechanism that assists in the detection of rogue access points. The feature has three components: (1) a radio frequency (RF) scanning task that runs on the Wireless AP, (2) an application called the Data Collector on the Summit WM Controller that receives and manages the RF scan messages sent by the Wireless AP, (3) an Analysis Engine on the Summit WM Controller that processes the scan data.
Wireless AP	The Wireless AP is a wireless LAN thin access point (IEEE 802.11) provided with unique software that allows it to communicate only with a Summit WM Controller. (A thin access point handles the radio frequency (RF) communication but relies on a controller to handle WLAN elements such as authentication.) The Wireless AP also provides local processing such as encryption. The Wireless AP is a dual-band access point, with 802.11a/b/g/n radios.
WM Access Domain Services (WM-AD)	The WM Access Domain Services (WM-AD) technique is Extreme Networks's means of mapping wireless networks to the topology of an existing wired network. When you set up WM Access Domain Services (WM-AD) on the Summit WM Controller, you are defining subnets for groups of wireless users. This WM-AD definition creates a virtual IP subnet where the Summit WM Controller acts as a default gateway for wireless devices. This technique enables policies and authentication to be applied to the groups of wireless users on a WM-AD, as well as the collecting of accounting information. When a WM-AD is set up on the Summit WM Controller, one or more Wireless APs (by radio) are associated with it. A range of IP addresses is set aside for the Summit WM Controller's DHCP server to assign to wireless devices.

A Summit WM Controller's physical description

This chapter describes the physical description and LED states of the following models of the Summit WM Controllers:

- Summit WM1000 Controller
- Summit WM100 Controller
- Summit WM200/2000 Controller
- Summit WM20 Controller

Summit WM1000 Controller front panel

The Summit WM Controller WM1000 doesn't have any component on the front panel except two LED lights. These two LED lights are:

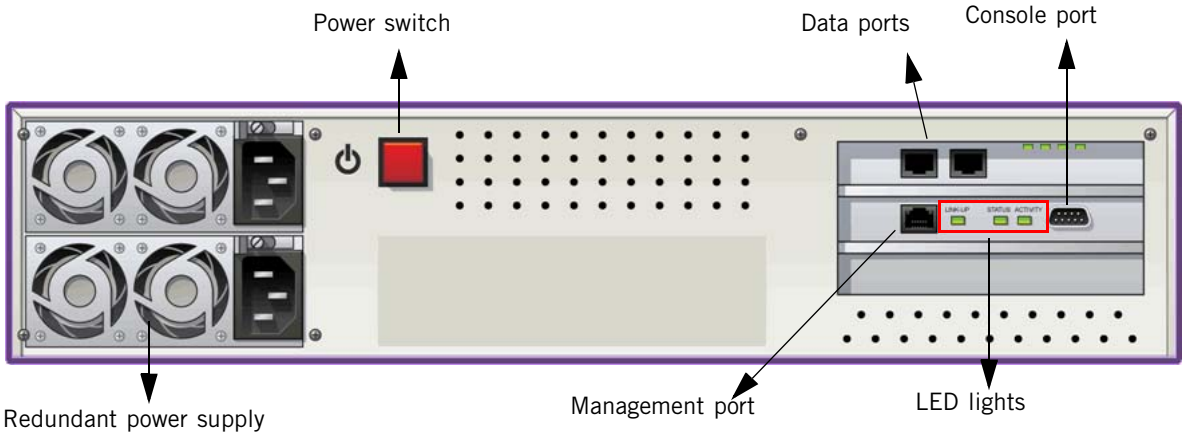
- STATUS LED - For more information, see the STATUS LED description in "Summit WM1000 Controller back panel" on page 327.
- ACTIVITY LED - For more information, see the ACTIVITY LED description in "Summit WM1000 Controller back panel" on page 327.

These two LED lights are also located on the back panel of the Summit WM Controller WM1000.

Summit WM1000 Controller back panel

The following figure identifies the main components on the back panel of Summit WM Controller WM1000.

Figure 24: Summit WM1000 Controller back panel



NOTE

The Summit WM1000 has a redundant power supply (two power supplies).

Summit WM1000 Controller data port cabling specification

The data ports have MT-RJ fiber optic connectors. Depending upon your network infrastructure, you must get any one of the following cables:

- MT-RJ connector to MT-RJ connector
- MT-RJ connector to SC connector
- MT-RJ connector to LC connector
- MT-RJ connector to any other connector that is appropriate for your infrastructure

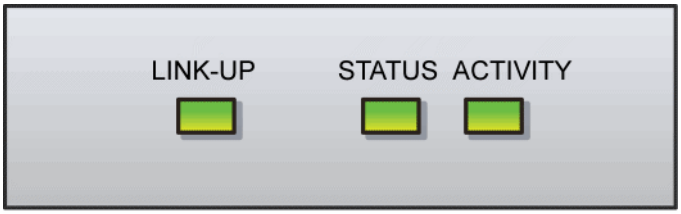
NOTE

If your infrastructure does not allow the optic fiber connection, you must get a Gigabit Media Converter to convert the fiber connection to a copper Gigabit connection. For example, you can use Netgear GC102 converter that receives the fiber connection and outputs traffic via the RJ45 copper port (Unshielded Twisted Pair - UTP).

Summit WM1000 Controller LEDs

The Summit WM1000 Controller has three LED lights on its back panel.

Figure 25: Summit WM1000 Controller LED Lights



The description of the LED states is provided below:

- LINK-UP LED - Displays the link status of management port Ethernet link as seen by the system's software. This LED is located only on the back panel of the Summit WM Controller WM1000.
- STATUS LED - Indicates the normal state of the Summit WM Controller as seen by the system's software. This LED covers all stages of the Summit WM Controller, ranging from restarting, to shutting-down. As long as the Summit WM Controller is running normally, this LED will remain lit. The STATUS LED is located on the back panel as well as the front panel.
- ACTIVITY LED - Indicates the amount of traffic carried to and from the Altitude APs. The ACTIVITY LED is located on the back panel as well as the front panel.

NOTE

When the system configuration is in progress, the Status and Activity LEDs pattern is as follows:
- Status LED is set to Amber and blinks on a two-second interval.
- Activity LED is set to Green.

Summit WM100 Controller front panel

The Summit WM100 Controller does not have any component on the front panel except two LED lights.

The description of the LED states is provided below:

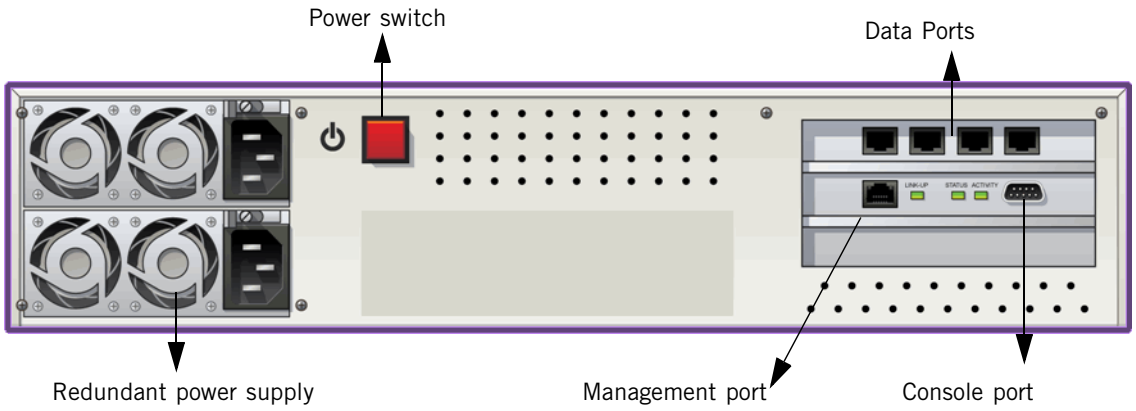
- STATUS LED - For more information, see the STATUS LED description in "Summit WM1000 Controller back panel" on page 327.
- ACTIVITY LED - For more information, see the ACTIVITY LED description in "Summit WM1000 Controller back panel" on page 327.

The STATUS LED is located on the back panel as well as the front panel of the Summit WM Controller WM100.

Summit WM100 Controller back panel

The following figure identifies the main components on the back panel of Summit WM Controller WM100.

Figure 26: Summit WM100 Controller back panel



NOTE

The Summit WM100 Controller has the same number of LED lights on the back panel as the Summit WM1000 Controller. The LED description of their state is also identical to WM100. For information on Summit WM100 Controller LEDs' states, see the descriptions of STATUS LED and ACTIVITY LED in "Summit WM1000 Controller back panel" on page 327.

NOTE

Summit WM100 Controller may have a standard power supply (one power supply) or a redundant power supply (two power supplies).

Summit WM100 Controller data port cabling specification

The Summit WM100 Controller data ports have copper connectors.

NOTE

If your infrastructure does not allow the copper connection, you must get a Gigabit Media Converter to convert the copper connection to a fibre optic connection. For example, you can use Netgear GC102 converter that receives the copper connection and outputs traffic via the fibre optic connector.

This appendix describes the physical description and LEDs, SSD codes and their description of the following models of the Summit WM Controller:

- Summit WM Controller WM200/2000
- Summit WM Controller WM20

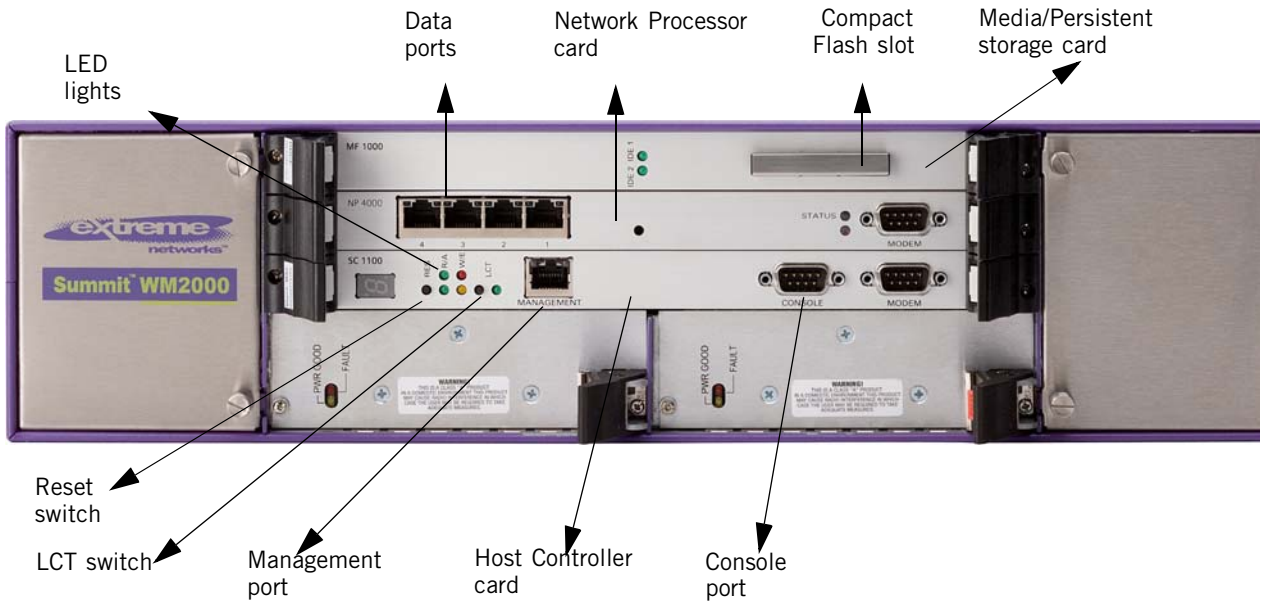
Summit WM200/2000 Controller front panel

The Summit WM200/2000 Controller is composed of the following three cards:

- Media/Persistent Storage Card
- Network Processor Card
- Host Summit WM Controller Card

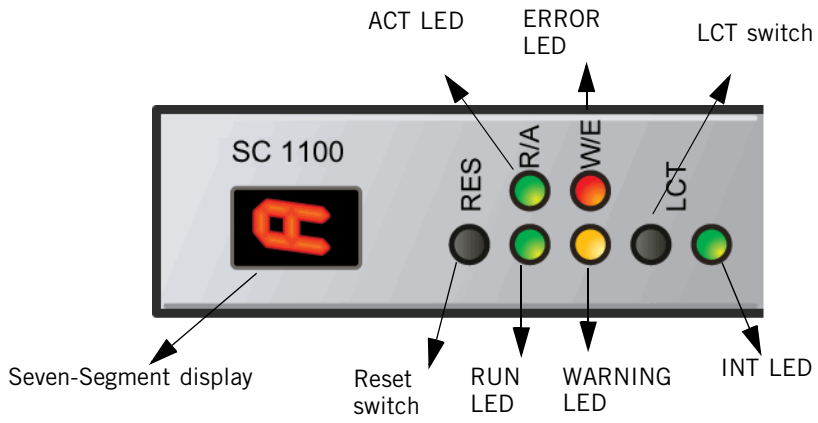
The following figure identifies the main components on the front panel of Summit WM200/2000 Controller.

Figure 27: Summit WM200/2000 Controller front panel



The Summit WM200/2000 Controller has five LED lights and two switches on its front panel.

Figure 28: Summit WM200/2000 Controller's LED lights and switches



The description of the LED states and switches is provided below:

- Reset Switch - Reboots the system.
- RUN LED - Indicates the CPU's initialization has completed and the system is ready to provide application level services.
- ACT LED - Indicates the system's software is in active running state.
- WARNING/ERROR LEDs - Indicate a problem in the running state of the system.
  - Whenever either of the alarm LEDs is lit, the seven-segment display provides the corresponding code point for the error indication. When the system is fully active and running, the console displays the letter **A** as seen in Figure 28.
- LCT Switch - The LCT button is used during the manufacturing process and is inactive otherwise.
- INT LED - Not used in the current release.

LED states and Seven Segment Display (SSD) codes

Firmware initialization:

Table 29: LED states and SSD codes during firmware initialization

Active LED	Warning LED	Error LED	SSD Codes	Condition
Green			0	The processor has started; and the firmware has taken control.
Green			3	The Host Controller Card has failed to download Bootloader from Flash.
Green			4	The system is checking firmware consistency.
Green			5	The system is formatting memory.
Green			6	The system is initializing load device. **Note:** If the SSD code is stuck at 6 for more than a minute, it implies that the Network Processor Card is installed in wrong slot.

Table 29: LED states and SSD codes during firmware initialization (Continued)

Active LED	Warning LED	Error LED	SSD Codes	Condition
Green			9	The system is loading subsystem.
Green			b	The system is starting the operation system. The system is active.

NOTE

Although the Active LED will be lit Green during the firmware initialization, this LED state is irrelevant to the SSD display or the condition. You must ignore the LED state during the firmware initialization.

Application initialization:

Table 30: LED states and SSD codes during application initialization

Active LED	Warning LED	Error LED	SSD Code	Condition
Green			0	Application initialization started.
Green			C	System configuration in progress
Green			1	Continuing application initialization
Green			2	Initializing Forwarding Engine
Green			3	Completing application initialization.
Green			A	Application initialization complete. System active.
Green			H	System halted. Administrator requested halting of system.

Warning conditions:

Table 31: LED states and SSD codes during warning conditions

Active LED	Warning LED	Error LED	SSD Code	Condition
Green	Yellow		1	High temperature reached.
Green	Yellow		2	Fan unit failure. Rotation counter indicates zero speed for one of the lateral trays. May be the result of fan tray removal.
Green	Yellow		3	Power supply failure. Failed to detect one of the power supplies. May be the result of the fan tray removal of one of the power supplies.
Green	Yellow		4	FDD low sector count (40 backup sectors remaining).
Green	Yellow		5	FDD extremely low sector count (20 backup sectors remaining)

Error conditions:

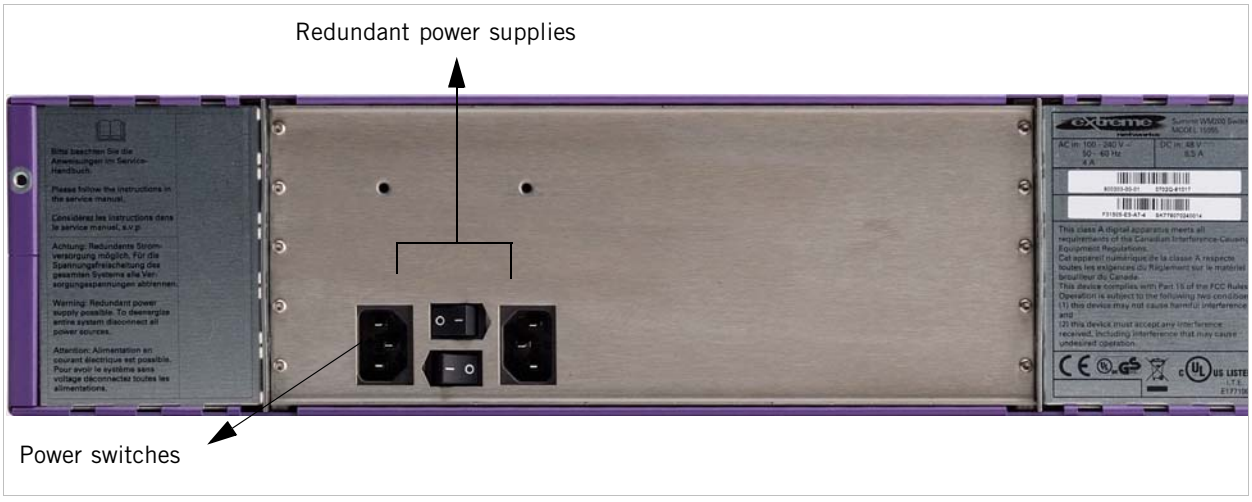
Table 32: LED states and SSD codes during error conditions

Active LED	Warning LED	Error LED	SSD Code	Condition
Green		Red	1	Failed to identify FDD. Possibly due to removal of FDD card.
Green		Red	2	Failed to initialize NPE card.
Green		Red	3	Critical threshold reached (95C for NPE). The system will reboot.
Green		Red	4	Full fan assembly failure (both trays). The system will reboot.
Green		Red	5	Application initialization failure. Startup manager failed to initialize all the components of the system. The system will reboot.
Green		Red	6	Lost connectivity with ethernet interface. Possible failure of NPE card. The system will reboot.
Green		Red	7	MF 1000 card failure. Backup sectors exhausted.
Green		Red	8	NP 4000 card initialization failure. Firmware self test (BIST) has detected failure in one or more components (memory, bus, interconnects)

Summit WM200/2000 Controller back panel

The following figure identifies the main components on the back panel of Summit WM200/2000 Controller.

Figure 29: Summit WM200/2000 Controller back panel



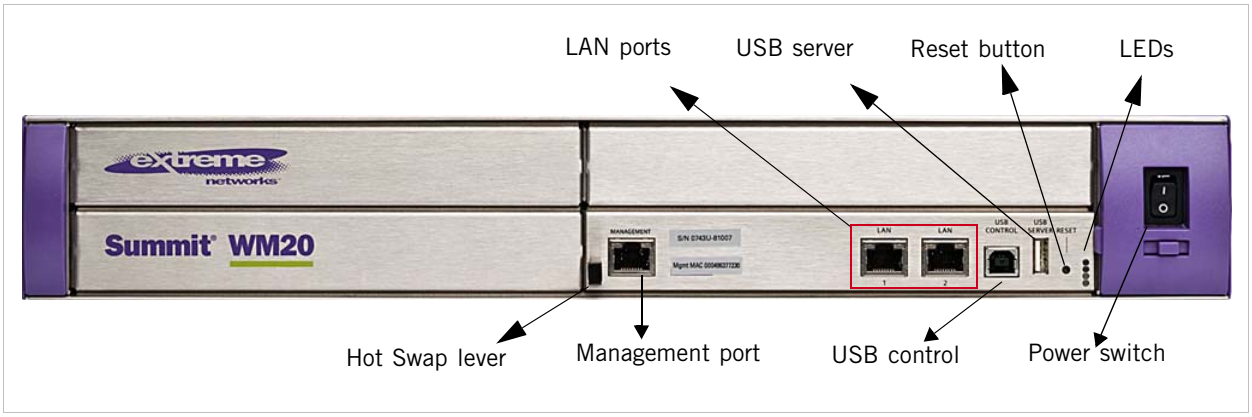
NOTE

The hardware for the Summit WM200 Controller and the Summit WM2000 Controller are identical.

Summit WM20 Controller

Summit WM20 Controller front panel

Figure 30: Summit WM20 Controller front panel

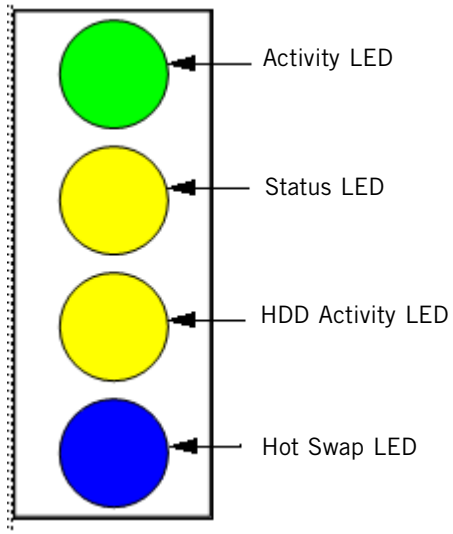


NOTE

The hot swap lever is not enabled in the current release. Pulling the hot swap lever will not affect the normal operation if the Summit WM20 Controller is already running. However, if you attempt to reboot the Summit WM20 Controller with the hot swap lever pulled out, the controller will fail to reboot. If you pull the hot swap lever while the Summit WM20 Controller is in operation, the Hot Swap LED will light up.

The Summit WM20 Controller has four lights on its front panel.

Figure 31: Summit WM20 Controller LED lights



The functional definitions of the Summit WM20 Controller's LEDs are provided below:

- ACTIVITY LED - Indicates the CPU activity, including the amount of traffic carried to and from the Altitude APs.

- STATUS LED - Indicates the normal state of the Summit WM Controller as seen by the system's software. This LED covers all stages of the Summit WM Controller, ranging from restarting, to shutting-down. As long as the Summit WM Controller is running normally, this LED will remain lit.

NOTE

When the system configuration is in progress, the Activity and Status LEDs are set to Amber and blink on a two-second interval.

- HDD Activity LED - Is hardware controlled to report Hard Drive Device (HDD) activity.
- Hot Swap LED - Indicates that the hot swap lever on the Summit WM Controller is pulled out.

Summit WM20 Controller's LED states

The description of the Summit WM20 Controller's LED states is provided below.

Figure 32: Summit WM20 Controller's LED states and their description

Status LED	Activity LED	Condition
Blinking Amber	Green	Power up (BIOS, POST)
Blinking Amber	Blinking Amber	System configuration in progress
Off	Green	System Booting (Failed to boot)
Off	Green	Start up Manager: Task Started
Solid Amber	Blinking Amber	Start up Manager: Task completes startup - All components active
Solid Amber	Blinking Green	A component fails to start or needs restarting. (Startup Manager Task Retrying that component)
Green	Blinking Red	Possible hardware failure (No more retries)
Solid Red	Off	A component fails (No more retries)
Blinking Red	Off	System about to reset by watchdog
Solid Red	Solid Red	System shutdown / Halt (Requires a manual reboot)

NOTE

LED 3 - HDD Activity LED - Orange / Amber
- HDD Activity LED is off when HDD is not in use
- HDD Activity LED is on when HDD is in use
LED 4 - Hot Swap LED - Blue
- Solid Blue when the hot swap button is pulled out

Summit WM20 Controller back panel

Figure 33: Summit WM20 Controller back panel

B Regulatory information

WARNING!

Warnings identify essential information. Ignoring a warning can lead to problems with the application.

This chapter provides the regulatory information for the following:

- "Summit WM Controller WM100/WM1000/WM20/WM200/2000" on page 338
- "Altitude 350-2 and Altitude 450/451" on page 339

The Summit WM AP models include:

- AP 350-2i/350-2d (AP35x series)
- Altitude AP 450/451(AP45x series)

NOTE

Throughout this appendix, the term "Altitude AP" refers to both AP models (AP35X series and AP45X series). Specific AP models are only identified in this appendix where it is necessary to do so.

NOTE

For technical specifications and certification information for the Outdoor AP, see the specific Siemens brand (SEN, A&D) Installation Guide.

Configuration of the Altitude AP frequencies and power output are controlled by the regional software license and proper selection of the country during initial installation and set-up. Customers are only allowed to select the proper country from their licensed regulatory domain related to that customer's geographic location, thus allowing the proper set-up of access points in accordance with local laws and regulations. The Altitude AP must not be operated until properly configured with the correct country setting or it may be in violation of the local laws and regulations.

WARNING!

Changes or modifications made to the Summit WM Controller or the Altitude APs which are not expressly approved by Extreme Networks could void the user's authority to operate the equipment.

Only authorized Extreme Networks service personnel are permitted to service the system. Procedures that should be performed only by Extreme Networks personnel are clearly identified in this guide.

NOTE

The Summit WM Controllers and the Altitude APs are in compliance with the European Directive 2002/95/EC on the restriction of the use of certain hazardous substances (RoHS) in electrical and electronic equipment.

Summit WM Controller WM100/WM1000/WM20/ WM200/2000

Conformance standards and directives

Safety

- UL 60950-1 (U.S)
- CSA C22.2 No.60950-01-03 (Canada)
- 2006/95/EC Low Voltage Directive (LVD)
- EN 60950-1 (Europe)
- IEC 60950-1 with applicable National Differences
- AS/NZS 60950.1 (Australia/New Zealand)

EMC (Emissions / Immunity)

- FCC Part 15, Subpart B, Class A (North America)
- ICES-003, Class A (Canadian Emissions)
- 89/336/EEC EMC Directive
- EN 55022 Class A (European Emissions)
- EN 55024 includes EN 61000-2,3,4,5,6,11 (European Immunity)
- EN 61000-3-2 (Harmonics)
- EN 61000-3-3 (Flicker)
- IEC/CISPR 22 Class A (International Emissions)
- IEC/CISPR 24 includes IEC/EN 61000-4-2,3,4,5,6,11 (International Immunity)
- Australia/New Zealand AS/NZS 3548 via EU standards (ACMA)

RoHS

- RoHS 6 compliant
- China RoHS compliant

Altitude 350-2 and Altitude 450/451

Country List for Altitude 450/451 Power Adapter

Power Adapter (PSC18U-480(A2)-R) can be operated in the countries indicated in Table 33.

Table 33: Country List for Altitude 450/451 Power Adapter (PSC18U-480(A2)-R)

Country	Volts	Frequency/Hertz
Argentina	220	50
Australia	240	50
Austria	230	50
Belgium	230	50
Belize	110	60
Bolivia	110/220	50
Canada	120	60
Chile	220	50
China	220	50
Colombia	110	60
Costa Rica	120	60
Czech Republic	220	50
Denmark	230	50
El Salvador	115	60
Estonia	220	50
Finland	230	50
France	230	50
Germany	230	50
Greece	230	50
Guatemala	120	60
Guinea	220	50
Guyana	110	60
Honduras	110	60
Hong Kong	220	50
Hungary	220	50
Iceland	220	50
India	220	50
Ireland	220	50
Italy	230	50
Japan	100	50/60
Korea	110/220	50/60
Latvia	220	50
Liechtenstein	220	50
Lithuania	220	50

Table 33: Country List for Altitude 450/451 Power Adapter (PSC18U-480(A2)-R)

Country	Volts	Frequency/Hertz
Luxembourg	230	50
Mexico	120	60
Netherlands	230	50
New Zealand	230	50
Nicaragua	120	60
Norway	230	50
Panama	120	60
Paraguay	220	50
Peru	110/220	50/60
Poland	220	50
Portugal	230	50
Russia	220	50
Singapore	230	50
Slovakia	220	50
Slovenia	220	50
Spain	230	50
Surinam	110/220	50/60
Sweden	230	50
Switzerland	230	50
United Kingdom	220	50
United States	120	60
Uruguay	220	50
Venezuela	120	60

Wi-Fi certification

Altitude 350-2 is Wi-Fi certified under Certification ID # WFA3822 for operation in accordance with IEEE802.11a/b/g standards. Altitude 350-2 APs come in two models. Altitude 350-2i is the model with integrated internal antennas. Altitude 350-2d comes with RP-SMA connectors for external antennas. It is shipped with two detached antennas. These Access Points are designed and intended to be used indoors.

Altitude 450 is Wi-Fi certified under Certification ID # WFA6124 for operation in accordance with IEEE 802.11a/b/g/draft n standards. Altitude 450 AP comes with internal integrated antennas.

Altitude 451 is Wi-Fi certified under Certification ID # WFA6125 for operation in accordance with IEEE 802.11a/b/g/draft n standards. Altitude 451 AP comes with RP-SMA connectors for use with external antennas. It is shipped with three paddle antennas.

Altitude 350-2/450/451 Access Points are designed and intended to be used indoors.

NOTE

Operation in the European Community and rest of the world may be dependant on securing local licenses, certifications, and regulatory approvals.

Altitude 350-2d external antenna AP

Optional approved 3rd party external antennas

The Altitude 350-2d external Antenna APs can also be used with optional certified external antennas:

- The external antennas on the 350-2d must be identical.
- Any unused antenna ports must be terminated when an external antenna is used with the Altitude 350-2d.

Antenna diversity

There are some limitations for using different antennas and Tx/Rx diversity:

- If **Alternate** antenna diversity is used for Tx or Rx, then the same antenna model must be used as left and right antennas. In addition, if cables are used to connect external antennas, the cables must be of the same length and similar attenuation. If these rules are not respected, antenna diversity will not function properly and there will be degradation in the link budget in both directions.
- You can choose to install only one antenna provided that both Tx and Rx diversity are configured to use that antenna and only that antenna. You can choose to install one antenna for 11b/g band and one antenna for 11a band, provided that the antenna diversity is configured appropriately on both radios.

Altitude 451 external antenna AP

Optional approved 3rd party external antennas

The Altitude 451 external antenna APs can also be used with optional certified external antennas:

- The external antennas on the Altitude 451 must be identical.
- Any unused antenna ports must be terminated when an external antenna is used with the Altitude 451.

United States

FCC Declaration of Conformity Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential and business environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause harmful interference, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment or devices.
- Connect the equipment to an outlet other than the receiver's.
- Consult a dealer or an experienced radio/TV technician for suggestions.

USA Conformance Standards

This equipment meets the following conformance standards:

Safety

- UL 60950-1
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code.

EMC

- FCC CFR 47 Part 15, Class B

Radio transceiver

- CFR 47 Part 15.247, Subpart C (2.4 GHz)
- CFR 47 Part 15.407, Subpart E (5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.311n (AP45x)
- IEEE 802.3af (PoE)

WARNING!

The Altitude APs must be installed and used in strict accordance with the manufacturer's instructions as described in this guide and related documentation for the device to which the Altitude AP is connected. Any other installation or use of the product violates FCC Part 15 regulations.

Operation of the Altitude AP is restricted for indoor use only, specifically in the UNII 5.15 - 5.25 GHz band in accordance with 47 CFR 15.407(e).

This Part 15 radio device operates on a non-interference basis with other devices operating at the same frequency when using antennas provided or other Extreme Networks certified antennas. Any changes or modification to the product not expressly approved by Extreme Networks could void the user's authority to operate this device.

For the product available in the USA market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.

FCC RF Radiation Exposure Statement

The Altitude AP complies with FCC RF radiated exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This device has been tested and has demonstrated compliance when simultaneously operated in the 2.4 GHz and 5 GHz frequency ranges. This device must not be co-located or operated in conjunction with any other antenna or transmitter.

CAUTION

The radiated output power of the Altitude AP is below the FCC radio frequency exposure limits as specified in "Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields" (OET Bullet 65, Supplement C). This equipment should be installed and operated with a minimum distance of 25 cm between the radiator and your body or other co-located operating antennas.

Altitude 350-2d/Altitude 451 optional 3rd party external antennas

The Altitude 350-2d/Altitude 451 external antenna APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested and approved for use with the external antenna models.

CAUTION

When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to Table 36 and Table 37.

Professional installation

To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)
- The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.

Table 34: List of FCC approved antennas - Altitude 350-2d

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type
Cushcraft							
#1	SR2405135 Dxxx	indoor	directional	5	2400-2500	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#2	S24493DSx xx	indoor	omni, 2 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.
#3	SL24513Px xx	indoor	omni	3	2400-2500 5150-5350	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#4	S24497Pxxx	indoor	directional	7	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
Hyperlink Tech							
#5	HG2458CUx xx	indoor	omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female
Maxrad							
#6	MDO24005 PTxxx	indoor	omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.

Table 35: List of FCC approved antennas - Altitude 451

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type	Total # required antennas
Cushcraft								
#1	SR249120D	indoor	120 degree sector directional	5	2400-2500 4900-5900	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3
#2	S24493TS	indoor	omni, 3 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 3ea.	1

Table 35: List of FCC approved antennas - Altitude 451 (Continued)

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type	Total # required antennas
#3	SL24513WP	indoor	omni	3	2400-2500 5150-5850	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3
#4	S24497Pxxx	indoor	60 degree sector directional	7 8	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3
Hyperlink Tech								
#5	HG2458CUxxx	indoor	omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female	3
Maxrad								
#6	MDO24005PTxxx	indoor	omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.	1

NOTE

The qualification testing and results are based on above described antennas, cable types, lengths, and connector types. Other cable lengths and connector types are also available which are specified by the suffix part of the part numbers (for example, SR2405135Dxxx, where the xxx suffix represents cable length and/or connector type). The antenna feedline used in testing are the minimum cable length. Longer cable may be used with losses greater than or equal to the cables used for testing. The maximum power settings must be adjusted according to Table 36 and Table 37.

NOTE

If one of the above antennas is used, you must select an operating channel (on the Altitude APs configuration pages) and the corresponding allowed max power from the values listed in Table 36 and Table 37. DO NOT select a higher power than the values listed in Table 36 and Table 37.

Table 36: Maximum channel power - Altitude 350-2d - FCC domain

Antenna			Antenna #1 Cushcraft SR2405135Dxxx	Antenna #2 Cushcraft S24493DSxxx	Antenna #3 Cushcraft SL24513Pxxx	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2400-2500	1-11	16	17	17	16	17	17
11g	2400-2500	1-11	14*	14*	14*	14*	14*	14*
11a	5150-5250	36-48	N/S	17	17	17	17	N/S
11a	5250-5350	52-64	N/S	18	18	18	18	N/S
11a	5470-5725	100-140	N/S	N/S	N/S	N/S	N/S	N/S
11a	5725-5850	149-165	N/S	14	N/S	14	14	N/S

CAUTION

** Due to regulatory restrictions, channel 1 on the Altitude 350-2d must be reduced to 10, 13, 13, 10, 12, and 13 dBm respectively for each antenna model.*

CAUTION

For antenna #3 (Cushcraft SL24513Pxxx) on the Altitude 350-2d do not select the Auto channel selection (on the Altitude APs configuration pages) for the 11a radio. Instead, only select a channel from the listed supported channels in Table 36.
Operating on a channel that is NOT supported (N/S) is in violation of the law.

Table 37: Maximum channel power - Altitude 451 - FCC domain

Antenna			Antenna #1 Cushcraft SR249120D	Antenna #2 Cushcraft S24493TS	Antenna #3 Cushcraft SL24513WP	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2400-2500	1-11	20	23	23	23	23	23

Table 37: Maximum channel power - Altitude 451 - FCC domain

Antenna			Antenna #1 Cushcraft SR249120D	Antenna #2 Cushcraft S24493TS	Antenna #3 Cushcraft SL24513WP	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005 PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11g	2400-2500	1-11	19	19	19	19	19	19
HT 20	2400-2500	1-11	17	20	20	19	18	20
HT 40	2400-2500	1-11	18	17	17	16	16	18
11a	5150-5250	36-48	16	16	16	16	16	N/S
HT 20	5150-5250	36-48	16	16	16	16	16	N/S
HT 40	5150-5250	36-48	15	15	15	15	15	N/S
11a	5250-5350	52-64	18	18	18	18	18	N/S
HT 20	5250-5350	52-64	18	18	18	18	18	N/S
HT 40	5250-5350	52-64	15	15	15	15	15	N/S
11a	5470-5725	100-140	18	18	18	18	18	N/S
HT 20	5470-5725	100-140	18	18	17	17	18	N/S
HT 40	5470-5725	100-140	16	16	16	16	16	N/S
11a	5725-5850	149-165	22	22	22	22	22	N/S
HT 20	5725-5850	149-165	22	22	22	22	22	N/S
HT 40	5725-5850	149-165	22	22	22	22	22	N/S

CAUTION

*Altitude 350-2d/Altitude 451 channels designated as N/S are not supported by the antenna and must not be selected from the **Altitude APs configuration** pages.*

CAUTION

When using the Auto channel selection in a mixed AP or mixed antenna environment, the maximum channel power must be 10dBm in the 2.4 GHz band and 14dBm in the 5 GHz band.

Table 38: Maximum channel power when using Auto channel selection - Altitude 350-2d - FCC domain

Antenna			Antenna #1 Cushcraft SR2405135Dxxx	Antenna #2 Cushcraft S24493DSxxx	Antenna #3 Cushcraft SL24513Pxxx	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-11	10	13	13	10	12	13
	5150-5850	36-165	N/S	14	17	14	14	N/S

Table 39: Maximum channel power when using Auto channel selection - Altitude 451 - FCC domain

Antenna			Antenna #1 Cushcraft SR249120D	Antenna #2 Cushcraft S24493TS	Antenna #3 Cushcraft SL24513WP	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-11	17	17	17	16	16	18
	5150-5850	36-48	15	15	15	15	15	N/S

CAUTION

*For both Altitude 350-2d/Altitude 451, if you select the **Auto** channel selection (on the **Altitude APs** configuration pages), you must also select the power values listed in Table 38 and Table 39. DO NOT select a higher power than the value listed in Table 38 and Table 39*

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

Canada

Industry Canada Compliance Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numerique respecte les limites de bruits radioelectriques applicables aux appareils numeriques de Classe B prescrites dans la norme sur le materiel brouilleur: "Appareils Numeriques," NMB-003 edictee par le Industrie Canada.

This device complies with Part 15 of the FCC Rules and Canadian Standard RSS-210. Operation is subject to the following conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.
- This Class B digital apparatus complies with Canadian ICES-003.
- Operation in the 5150-5250 MHz band is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
- Please note that high power radars are allocated as primary users (meaning they have priority) and can cause interference in the 5250-5350 MHz and 5470-5725 MHz bands of LE-LAN devices.
- For the product available in the Canadian market, only channels 1 to 11 can be operated. Selection of other channels in the 2.4 GHz band is not possible.
- The maximum antenna gain permitted for the AP35X operating in the 5250-5350 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the default external antenna that is shipped with the unit. To comply with the e.i.r.p. limit with the optional external antennas, refer to Table 40.
- The maximum antenna gain permitted for the AP35X operating in the 5725-5825 MHz band to comply with the e.i.r.p. limit is 4.3 dBi for the internal antenna and 5 dBi for the default external antenna that is shipped with the unit. To comply with the e.i.r.p. limit with the optional external antennas, refer to Table 40.
- The maximum antenna gain permitted for the AP45X operating in bands 5250-5350 MHz and 5470-5725 MHz to comply with the e.i.r.p. limit is 6 dBi for the internal antenna and 5 dBi for the external antenna.
- The maximum antenna gain permitted for the AP45X operating in the 5725-5825 MHz band to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate is 6 dBi for the internal antenna and 5 dBi for the external antenna.

Canada Conformance Standards

This equipment meets the following conformance standards:

Safety

- C22.2 No.60950-1-03
- UL 2043 Plenum Rated as part of UL 60950-1. Suitable for use in environmental air space in accordance with Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1

EMC

- ICES-003, Class B

Radio transceiver

- RSS-210 (2.4 GHz and 5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP45x)
- IEEE 802.3af (PoE)

Altitude 350-2d/Altitude 451 optional 3rd party external antennas

The Altitude 350-2d/Altitude 451 external antenna APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested with and approved for use with the external antenna model.

CAUTION

When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to Table 42 and Table 43.

Professional installation

This device must be professionally installed. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)

The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.

Table 40: List of IC approved antennas - Altitude 350-2d

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type
Cushcraft							
#1	SR2405135 Dxxx	indoor	Directional	5	2400-2500	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#2	S24493DSx xx	indoor	Omni, 2 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.
#3	SL24513Pxx x	indoor	Omni	3	2400-2500 5150-5350	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#4	S24497Pxxx	indoor	Directional	7	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
Hyperlink Tech							
#5	HG2458CUx xx	indoor	Omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female
Maxrad							
#6	MDO24005 PTxxx	indoor	Omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.

Table 41: List of IC approved antennas - Altitude 451

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type	Total # required antennas
Cushcraft								
#1	SR249120D	indoor	120 degree sector directional	5	2400-2500 4900-5900	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3

Table 41: List of IC approved antennas - Altitude 451 (Continued)

#	Model	Application	Shape	Gain (dBi)	Frequency (MHz)	Coax Cable Length/Type	Connector Type	Total # required antennas
#2	S24493TS	indoor	omni, 3 inputs	3	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 3ea.	1
#3	SL24513WP	indoor	omni	3	2400-2500 5150-5850	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3
#4	S24497Pxxx	indoor	60 degree sector directional	7 8	2400-2500 4900-5990	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA	3
Hyperlink Tech								
#5	HG2458CUxxx	indoor	omni	3	2300-2600 4900-6000	1 foot / 20AWG Coleman Cable 921021	N-female	3
Maxrad								
#6	MDO24005PTxxx	indoor	omni, 2 inputs	5.2	2400-2485	3 feet / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2ea.	1

NOTE

The qualification testing and results are based on above described antennas, cable types, lengths, and connector types. Other cable lengths and connector types are also available which are specified by the suffix part of the part numbers (ex. SR2405135Dxxx, where the xxx suffix represents cable length and/or connector type). The antenna feedline used in testing are the minimum cable length. Longer cable may be used with losses greater than or equal to the cables used for testing. The maximum power settings must be adjusted according to Table 42 and Table 43.

NOTE

*If one of the above antennas is used, you must select an operating channel (on the **Altitude APs** configuration pages) and the corresponding allowed max power from the values listed in Table 42 and Table 43. DO NOT select a higher power than the value listed in Table 42 and Table 43.*

Table 42: Maximum channel power - Altitude 350-2d - IC domain

Antenna			Antenna #1 Cushcraft SR2405135Dxxx	Antenna #2 Cushcraft S24493DSxxx	Antenna #3 Cushcraft SL24513Pxxx	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2400-2500	1-11	16	17	17	16	17	17
11g	2400-2500	1-11	14*	14*	14*	14*	14*	14*
11a	5150-5250	36-48	N/S	17	17	17	17	N/S
11a	5250-5350	52-64	N/S	18	18	18	18	N/S
11a	5470-5725	100-140	N/S	N/S	N/S	N/S	N/S	N/S
11a	5725-5850	149-165	N/S	14	N/S	14	14	N/S

CAUTION

** Due to regulatory restrictions, channel 1 on the Altitude 350-2d must be reduced to 10, 13, 13, 10, 12, and 13 dBm respectively for each antenna model.*

CAUTION

For antenna #3 (Cushcraft SL24513Pxxx) on the Altitude 350-2d, do not select the Auto channel selection (on the Altitude APs configuration pages) for the 11a radio. Instead, only select a channel from the listed supported channels in Table 42.
Operating on a channel that is NOT supported (N/S) is in violation of the law.

Table 43: Maximum channel power - Altitude 451 - IC domain

Antenna			Antenna #1 Cushcraft SR249120D	Antenna #2 Cushcraft S24493TS	Antenna #3 Cushcraft SL24513WP	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2400-2500	1-11	20	23	23	23	23	23
11g	2400-2500	1-11	19	19	19	19	19	19

Table 43: Maximum channel power - Altitude 451 - IC domain (Continued)

Antenna	Frequency range (MHz)	Channel range	Antenna #1 Cushcraft SR249120D Power limit (dBm)	Antenna #2 Cushcraft S24493TS Power limit (dBm)	Antenna #3 Cushcraft SL24513WP Power limit (dBm)	Antenna #4 Cushcraft S24497Pxxx Power limit (dBm)	Antenna #5 Hyperlink Tech HG2458CUxxx Power limit (dBm)	Antenna #6 Maxrad MD024005PTxxx Power limit (dBm)
HT 20	2400-2500	1-11	17	20	20	19	18	20
HT 40	2400-2500	1-11	18	17	17	16	16	18
11a	5150-5250	36-48	16	16	16	16	16	N/S
HT 20	5150-5250	36-48	16	16	16	16	16	N/S
HT 40	5150-5250	36-48	15	15	15	15	15	N/S
11a	5250-5350	52-64	18	18	18	18	18	N/S
HT 20	5250-5350	52-64	18	18	18	18	18	N/S
HT 40	5250-5350	52-64	15	15	15	15	15	N/S
11a	5470-5725	100-140	18	18	18	18	18	N/S
HT 20	5470-5725	100-140	18	18	17	17	18	N/S
HT 40	5470-5725	100-140	16	16	16	16	16	N/S
11a	5725-5850	149-165	22	22	22	22	22	N/S
HT 20	5725-5850	149-165	22	22	22	22	22	N/S
HT 40	5725-5850	149-165	22	22	22	22	22	N/S

CAUTION

*Altitude 350-2d/Altitude 451 channels designated as N/S are not supported by the antenna and must not be selected from the **Altitude APs** configuration pages.*

CAUTION

*For both Altitude 350-2d/Altitude 451, if you select the **Auto** channel selection (on the **Altitude APs** configuration pages) you must also select the power values listed in Table 44 and Table 45. DO NOT select a higher power than the value listed in Table 44 and Table 45.*

Table 44: Maximum channel power when using Auto channel selection - Altitude 350-2d - IC domain

Antenna			Antenna #1 Cushcraft SR2405135 Dxxxxxx	Antenna #2 Cushcraft S24493DSx xxxxx	Antenna #3 Cushcraft SL24513Pxx xxxx	Antenna #4 Cushcraft S24497Pxxx xxx	Antenna #5 Hyperlink Tech HG2458CUx xx	Antenna #6 Maxrad MD024005P Txxxxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-11	10	13	13	10	12	13
	5150-5850	36-165	N/S	14	17	14	14	N/S

Table 45: Maximum channel power when using Auto channel selection - Altitude 451 - IC domain

Antenna			Antenna #1* Cushcraft SR249120D	Antenna #2* Cushcraft S24493TS	Antenna #3 Cushcraft SL24513WP	Antenna #4 Cushcraft S24497Pxxx	Antenna #5 Hyperlink Tech HG2458CUxxx	Antenna #6 Maxrad MD024005PTxxx
	Frequency range (MHz)	Channel range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-11	17	17	17	16	16	18
	5150-5850	36-48	15	15	15	15	15	N/S

CAUTION

When using the Auto channel selection in a mixed AP or mixed antenna environment, the maximum channel power must be 10dBm in the 2.4 GHz band and 14dBm in the 5 GHz band.

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

European community

The Altitude APs are designed for use in the European Union and other countries with similar regulatory restrictions where the end user or installer is allowed to configure the Altitude AP for operation by entry of a country code relative to a specific country. Upon connection to the controller, the software will prompt the user to select a country code. After the country code is selected, the controller will set up the Altitude AP with the proper frequencies and power outputs for that country code.

Although outdoor use may be allowed and may be restricted to certain frequencies and/or may require a license for operation, the Altitude 350-2i/350-2d AP is intended for indoor use and must be installed in a proper indoor location. Use the installation utility provided with the controller software to ensure proper set-up in accordance with all European spectrum usage rules. Contact local Authority for procedure to follow and regulatory information. For more details on legal combinations of frequencies, power levels and antennas, contact Extreme Networks.

Declaration of Conformity with R&TTE Directive of the European Union 1999/5/EC

The following symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

Declaration of Conformity in Languages of the European Community

English	Hereby, Extreme Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Extreme Networks vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Extreme Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart Extreme Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Extreme Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Extreme Networks déclare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Swedish	Härmed intygar Extreme Networks att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Extreme Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Extreme Networks die Übereinstimmung des "WLAN Wireless Controller bzw. Access Points" mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Extreme Networks ΔΗΛΩΝΕΙ ΟΤΙ Radio LAN device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Icelandic	Extreme Networks lysir her med yfir að thessi bunadur, Radio LAN device, uppfyllir allar grunnkrofur, sem gerdar eru i R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Extreme Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Extreme Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	Extreme Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Extreme Networks, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

New Member States requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Extreme Networks seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Extreme Networks nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Slovak	Extreme Networks týmto vyhlasuje, že Radio LAN device spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Extreme Networks tímto prohlašuje, že tento Radio LAN device je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.'
Slovenian	Šiuo Extreme Networks deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar ðo Extreme Networks deklarç, ka Radio LAN device atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem
Lithuanian	Extreme Networks deklaruoja, kad Radio LAN device atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas'.
Polish	Niniejszym, Extreme Networks, deklarujê, ¿e Radio LAN device spe³nia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

European conformance standards

This equipment meets the following conformance standards:

Safety

- 2006/95/EC Low Voltage Directive (LVD)
- IEC/EN 60950-1 + National Deviations

EMC (Emissions / Immunity)

- 89/336/EEC EMC Directive
- EN 55011/CISPR 11, Class B, Group 1 ISM
- EN 55022/CISPR 22, Class B
- EN 55024/CISPR 24, includes IEC/EN 61000-4-2,3,4,5,6,11
- EN 61000-3-2 and -3-3 (Harmonics and Flicker)
- EN 60601-1-2 (EMC immunity for medical equipment)
- EN 50385 (EMF)
- ETSI/EN 301 489-1 & -17

Radio transceiver

- R&TTE Directive 1999/5/EC
- ETSI/EN 300 328 (2.4 GHz)
- ETSI/EN 301 893 (5 GHz)

Other

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP45x)
- IEEE 802.3af (PoE)

RoHS

- European Directive 2002/95/EC

Altitude 350-2d/Altitude 451 optional 3rd party external antennas

The Altitude 350-2d/Altitude 451 external antenna APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities. The following optional antennas have been tested with and approved for use with the external antenna model.

CAUTION

When using an approved 3rd party external antenna (other than the default), the power must be adjusted according to Table 47 and Table 48.

Professional installation

This device must be professionally installed. The following are the requirements of professional installation:

- The device cannot be sold retail to the general public or by mail order. It must be sold to dealers.
- Installation must be controlled.
- Installation must be carried out by licensed professionals (equipment sold to dealers who hire installers)
- Installation requires special training (special programming and antenna and cable installations)

The intended use is generally not for the general public. Instead, it is generally for industry/commercial use.

Table 46: List of ETSI approved antennas - Altitude 350-2d and Altitude 451

#	Model	Location	Type	Gain (dBi)	Frequency (MHz)
			Huber+Suhner		
#1	SOA 2454/360/7/20/DF	outdoor-capable	omni	6 8	2400-2500 4900-5875
#2	SPA 2456/75/9/0/DF	outdoor-capable	planar 2 or 1 inputs	9	2400-2500 5150-5875
#3	SPA 2400/80/9/0/DS	outdoor-capable	planar 2 inputs	8.5	2300-2500

Table 46: List of ETSI approved antennas - Altitude 350-2d and Altitude 451 (Continued)

#	Model	Location	Type	Gain (dBi)	Frequency (MHz)
#4	SWA 0859/360/4/10/V	outdoor-capable	omni	7	2400-2500 4900-5875
#5	SOA 2400/360/4/0/DS	outdoor-capable	Omni	3.5	2400-2500
#6	SPA 2400/40/14/0/DS	outdoor-capable	planar 2 inputs	13.5	2400-2500
#7	SWA 2459/360/4/45/V	outdoor-capable	omni	>4	2400-5875

NOTE

*If one of the above antennas is used, you must select an operating channel (on the **Altitude APs** configuration pages) and the corresponding allowed max power from the values listed in Table 47 and Table 48. DO NOT select a higher power than the value listed in Table 47 and Table 48.*

Table 47: Maximum channel power - Altitude 350-2d - ETSI domain

Antenna	Frequency (MHz)	Ch. range	Antenna #1 Huber +Suhner SOA 2454/ 360/7/20/ DF Power limit (dBm)	Antenna #2 Huber +Suhner SPA 2456/75/ 9/0/DF Power limit (dBm)	Antenna #3 Huber +Suhner SPA 2400/ 80/9/0/DS Power limit (dBm)	Antenna #4 Huber +Suhner SWA 0859/ 360/4/10/ V Power limit (dBm)	Antenna #5 Huber +Suhner SOA 2400/ 360/4/0/ DS Power limit (dBm)	Antenna #6 Huber +Suhner SPA 2400/ 40/14/0/DS Power limit (dBm)	Antenna #7 Huber +Suhner SWA 2459/ 360/4/45/V Power limit (dBm)
11b	2400-2500	1-13	15	14	14	15	15	9	15
11g	2400-2500	1-13	15	13	13	15	15	9	15
11a	5150-5350	36-64	16	16	N/S	16	N/S	N/S	16
11a	5470-5725	100-140	20	19	N/S	20	N/S	N/S	20

Table 48: Maximum channel power - Altitude 451 - ETSI domain

Antenna			Antenna #1 Huber +Suhner SOA 2454/ 360/7/20/ DF	Antenna #2 Huber +Suhner SPA 2456/75/ 9/0/DF	Antenna #3 Huber +Suhner SPA 2400/80/ 9/0/DS	Antenna #4 Huber +Suhner SWA 0859/360/ 4/10/V	Antenna #5 Huber +Suhner SOA 2400/ 360/4/0/ DS	Antenna #6 Huber +Suhner SPA 2400/ 40/14/0/DS	Antenna #7 Huber +Suhner SWA 2459/ 360/4/45/ V
	Frequency (MHz)	Ch. range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
11b	2400-2500	1-13	15	16	15	13	16	9	16
11g	2400-2500	1-13	16	16	15	15	16	9	16
HT20	2400-2500	1-13	16	17	15	15	17	9	17
HT40	2400-2500	1-13	16	17	15	15	17	9	17
11a	5150-5350	36-64	18	18	N/S	18	N/S	N/S	18
HT20	5150-5350	36-64	17	17	N/S	17	N/S	N/S	17
HT40	5150-5350	36-64	17	17	N/S	17	N/S	N/S	17
11a	5470-5725	100-140	22	22	N/S	22	N/S	N/S	22
HT20	5470-5725	100-140	22	22	N/S	22	N/S	N/S	22
HT40	5470-5725	100-140	20	20	N/S	20	N/S	N/S	20

CAUTION

*Channels designated as N/S are not supported by the antenna and must not be selected from the **Altitude APs** configuration pages.*

CAUTION

*If you select the **Auto** channel selection (on the **Altitude APs** configuration pages), you must also select the power values listed in Table 49 and Table 50. DO NOT select a higher power than the value listed in Table 49 and Table 50.*

Table 49: Maximum channel power when using Auto channel selection - Altitude 350-2d - ETSI domain

Antenna			Antenna #1 Huber +Suhner SOA 2454/ 360/7/20/DF	Antenna #2 Huber +Suhner SPA 2456/75/ 9/0/DF	Antenna #3 Huber +Suhner SPA 2400/ 80/9/0/DS	Antenna #4 Huber +Suhner SWA 0859/ 360/4/10/ V	Antenna #5 Huber +Suhner SOA 2400/ 360/4/0/ DS	Antenna #6 Huber +Suhner SPA 2400/40/ 14/0/DS	Antenna #7 Huber +Suhner SWA 2459/ 360/4/45/V
	Frequency (MHz)	Ch. range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-13	15	13	13	15	15	9	15
	5150-5725	36-140	16	16	N/S	16	N/S	N/S	16

Table 50: Maximum channel power when using Auto channel selection - Altitude 451 - ETSI domain

Antenna			Antenna #1 Huber +Suhner SOA 2454/ 360/7/20/ DF	Antenna #2 Huber +Suhner SPA 2456/75/ 9/0/DF	Antenna #3 Huber +Suhner SPA 2400/80/ 9/0/DS	Antenna #4 Huber +Suhner SWA 0859/ 360/4/10/ V	Antenna #5 Huber +Suhner SOA 2400/ 360/4/0/ DS	Antenna #6 Huber +Suhner SPA 2400/40/ 14/0/DS	Antenna #7 Huber +Suhner SWA 2459/ 360/4/45/V
	Frequency (MHz)	Ch. range	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)	Power limit (dBm)
	2400-2500	1-13	15	16	15	13	16	9	16
	5150-5725	36-140	17	17	N/S	17	N/S	N/S	17

CAUTION

When using the Auto channel selection in a mixed AP or mixed antenna environment, the maximum channel power must be 9dBm in the 2.4 GHz band and 16dBm in the 5 GHz band.

RF safety distance

The antennas used for this transmitter must be installed to provide a separation distance of at least 25 cm from all persons and must not be co-located or operating in conjunction with another antenna or transmitter.

Conditions of use in the European community

The Altitude APs with internal and external antennas are designed and intended to be used indoors. Some EU countries allow outdoor operation with limitations and restrictions, which are described in this section. It is the responsibility of the end user to ensure operation in accordance with these rules, frequencies, and transmitter power output. The Altitude AP must not be operated until properly configured for the customer's geographic location.

CAUTION

The user or installer is responsible to ensure that the Altitude AP is operated according to channel limitations, indoor / outdoor restrictions, license requirements, and within power level limits for the current country of operation. A configuration utility has been provided with the Summit WM Controller to allow the end user to check the configuration and make necessary configuration changes to ensure proper operation in accordance with the spectrum usage rules for compliance with the European R&TTE directive 1999/5/EC.

The Altitude APs with internal and external antennas are designed to be operated only indoors within all countries of the European Community. Some countries require limited channels of operation. These restrictions are described in this section.

CAUTION

The Altitude AP is completely configured and managed by the Summit WM Controller connected to the network. Please follow the instructions in this user guide to properly configure the Altitude APs.

- The Altitude APs require the end user or installer to ensure that they have a valid license prior to operating the Altitude AP. The license contains the region and the region exposes the country codes which allow for proper configuration in conformance with European National spectrum usage laws

- There is a default group of settings that each Altitude AP receives when it connects to the controller. There is the ability to change these settings. The user or installer is responsible to ensure that each Altitude AP is properly configured.

- The software within the controller will automatically limit the allowable channels and output power determined by the selected country code. Selecting the incorrect country of operation or identifying the proper antenna used, may result in illegal operation and may cause harmful interference to other systems.

- This device employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.

- The 5 GHz Turbo Mode feature is not enabled for use on the Altitude APs.

- The Auto channel setting of the 5 GHz described in this user guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements.

- The 5150-5350 MHz band, channels 36, 40, 44, 48, 52, 56, 60, or 64, are restricted to indoor use only.

- The external antenna APs must only use the antennas that are certified by Extreme Networks.

- The 2.4 GHz band, channels 1 - 13, may be used for indoor or outdoor use but there may be some channel restrictions.

- In Greece and Italy, the end user must apply for a license from the national spectrum authority to operate outdoors.

- In Belgium, outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.

- In France, outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7.

European spectrum usage rules

The AP configured with approved internal or external antennas can be used for indoor and outdoor transmissions throughout the European community as shown in the Table 51. Some restrictions apply in Belgium, France, Greece, and Italy.

Table 51: European spectrum usage rules

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 120,124,128,132,136, 140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Austria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Belgium	Indoor only	Indoor only	Indoor or outdoor *	Indoor only
Bulgaria	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Denmark	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Croatia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Cyprus	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Czech Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Estonia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Finland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
France	Indoor only	Indoor only	Indoor or outdoor	Indoor ch. 1-13 Outdoor 1-7 only
Germany	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Greece	Indoor only	Indoor only	Indoor (Outdoor w/License)	Indoor (Outdoor w/license)
Hungary	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Iceland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Ireland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Italy	Indoor only	Indoor only	Indoor or outdoor	Indoor (Outdoor w/license)
Latvia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Liechtenstein	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Lithuania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Luxembourg	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Netherlands	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Malta	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Norway	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Poland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Portugal	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Romania	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

Table 51: European spectrum usage rules

Country	5.15-5.25 (GHz) Channels: 36,40,44,48	5.25-5.35 (GHz) Channels: 52,56,60,64	5.47-5.725 (GHz) Channels: 100,104,108,112,116, 120,124,128,132,136, 140	2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)
Slovak Rep.	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Slovenia	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Spain	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Sweden	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Switzerland	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor
Turkey	Indoor only	Indoor only	n/a	Indoor or outdoor
U.K	Indoor only	Indoor only	Indoor or outdoor	Indoor or outdoor

NOTE

** Belgium requires notifying the spectrum agency if deploying > 300 meter wireless links in outdoor public areas.*

Certifications of other countries

The Altitude APs have been certified for use in various other countries. When the Altitude AP is connected to the Extreme Networks Summit WM controller, the user is prompted to select a country code. Once the correct country code is selected, the controller automatically sets up the Altitude AP with the proper frequencies and power outputs for that country code.

NOTE

It is the responsibility of the end user to select the proper country code for the country the device will be operated within or run the risk violating local laws and regulations.

Optional 3rd party external antennas

The external antenna Altitude APs can also be used with optional certified 3rd party antennas. However, in order to comply with the local laws and regulations, an approval may be required by the local regulatory authorities.

Other country specific compliance standards, approvals and declarations

Australia and New Zealand

- IEC 60950-1 CB Scheme + National Deviations
- AS/NZS 60950.1 (Safety)
- AS/NZS 3548 (Emissions via EU standards - ACMA)
- AS/NZS 4288 (Radio via EU standards)
- EN 300 328 (2.4 GHz)

- EN 301 893 (5 GHz)
- EN 301 489-1 & -17 (RLAN)
- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2.4 GHz)
- IEEE 802.11n (AP45X)
- IEEE 802.3af (PoE)

C SpectraLink Wireless Telephones

The Summit WM LAN Solution, consisting of the Summit WM Controller, Altitude APs, and the Summit WM Software, seamlessly integrates with SpectraLink Wireless Telephones to serve mobile voice and data requirements. The standards-based architecture of Summit WM LAN provides an exceptional infrastructure for voice quality and handset-reliability to the SpectraLink telephones.

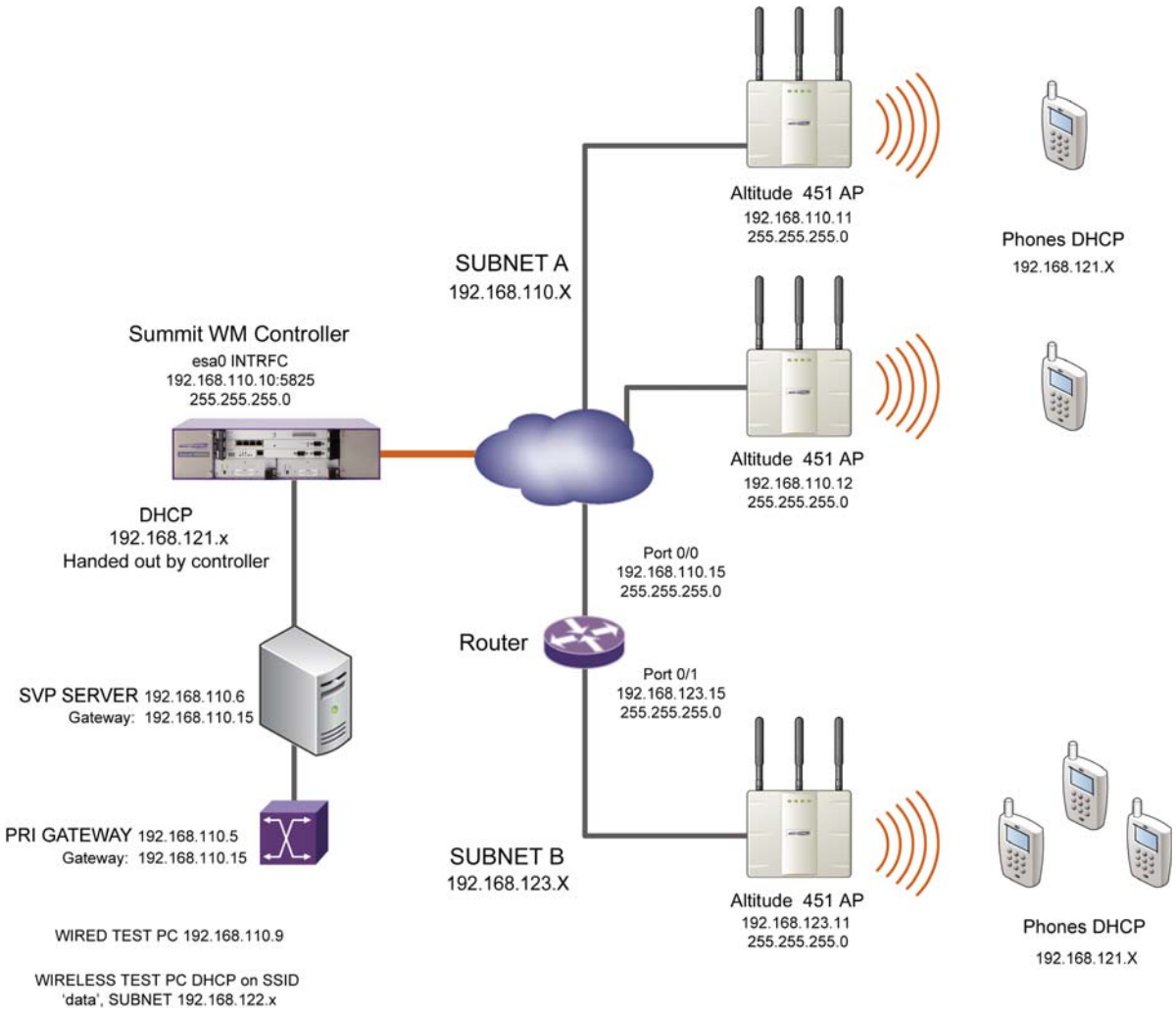
This appendix includes the following sections:

- "Network Topology" on page 368
- "Configuring Summit WM Controller for SpectraLink Telephones" on page 369

Network Topology

The following image depicts a typical network topology for SpectraLink telephones.

Figure 34: SpectraLink Network Topology



NOTE

The network topology depicted in Figure 34 is a dedicated network for SpectraLink Telephones. Other topologies are supported and can be used as required.

NOTE

For a successful deployment, all the network elements in the SpectraLink network should be provisioned to prioritize voice data.

Configuring Summit WM Controller for SpectraLink Telephones

This section describes how to configure the Summit WM Controller and Altitude APs for use with SpectraLink Wireless Telephones.

You have to configure the following features in the Summit WM Controller to set it up for SpectraLink telephones:

- Radio properties
- SSID
- Filters
- Multicast configuration
- Security
- Quality of Service (QoS)

NOTE

The configuration process for SpectraLink telephones applies identically to Summit WM APs, Outdoor APs and Altitude 802.11n APs, unless specified otherwise.

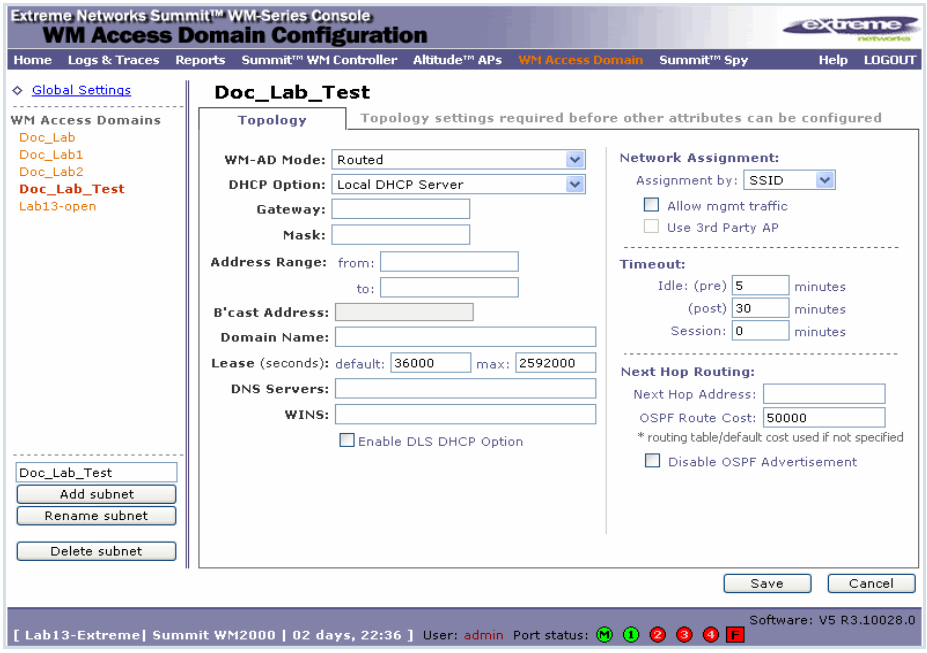
Setting up SSID

To set up the SSID:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 In the left pane, type a name that will identify the new WM-AD in the **Add subnet** box.

3 Click **Add subnet**. The name is displayed in the **WM-AD** list. The **Topology** tab is displayed.



4 From the **WM-AD Mode** drop-down menu, select the appropriate WM-AD mode:

NOTE

*It is recommended that you should choose **Bridge Traffic Locally at WM-AD** for SpectraLink network deployment.*

5 From the **DHCP Option** drop-down menu, you can select either the **Local DHCP Server** or **Use DHCP Relay**, depending upon your network topology.

6 In the **Gateway** box, type the network gateway address.

7 In the **Mask** box, type the appropriate values.

8 In the **Address Range** boxes (**from** and **to**), type the IP address range.

9 From the **Assignment Type** drop-down menu, select **SSID**.

10 Under **Timeout** section, type **2** in the **pre** and **post** boxes.

11 Under **Next Hop Routing** section, type **50000** in the **OSPF Route Cost** box.

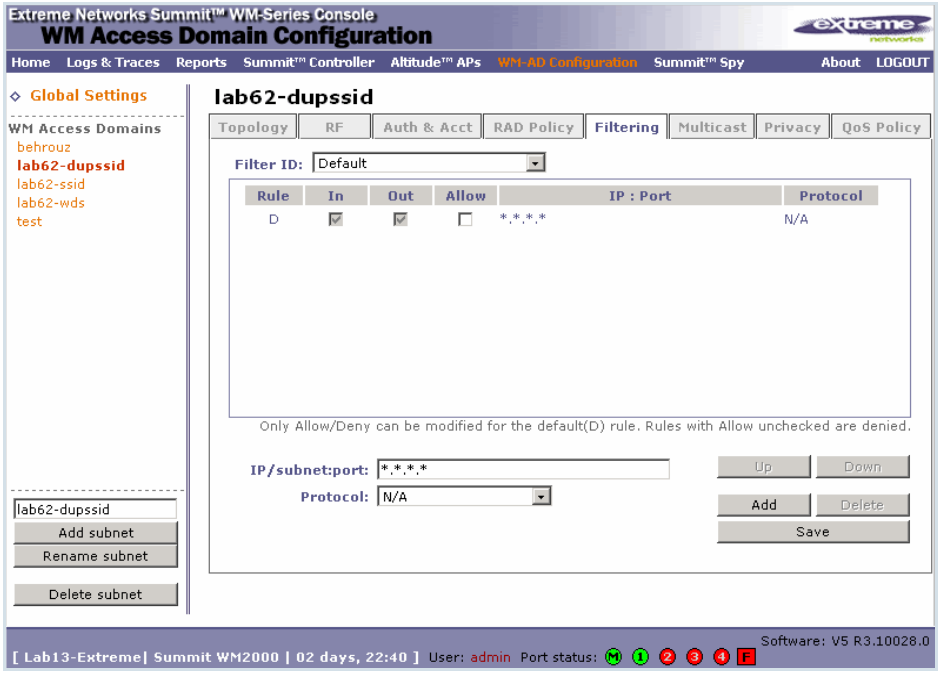
12 Click **Save**.

Configuring filters

To configure the filters:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 On the **WM Access Domain Configuration** screen, click the **Filtering** tab. The filtering rule for the **Default** filter is displayed in the centre pane.



3 Type the IP address of SVP server in **IP/Subnet:port** box.

4 From the **Protocol** drop-down menu, select **UDP**.

5 Click **Add**. The new filtering rule for the SVP server is displayed in the centre pane.

6 Click **Up**. The filtering rule for the SVP server moves up, before the filter rule for **Default** filter.

7 Type the IP address of SpectraLink Gateway in **IP/Subnet:port** box, and then repeat steps 4 to 6.

8 Add the filtering rules for the IP addresses of all network elements as explained in steps 3 to 6.

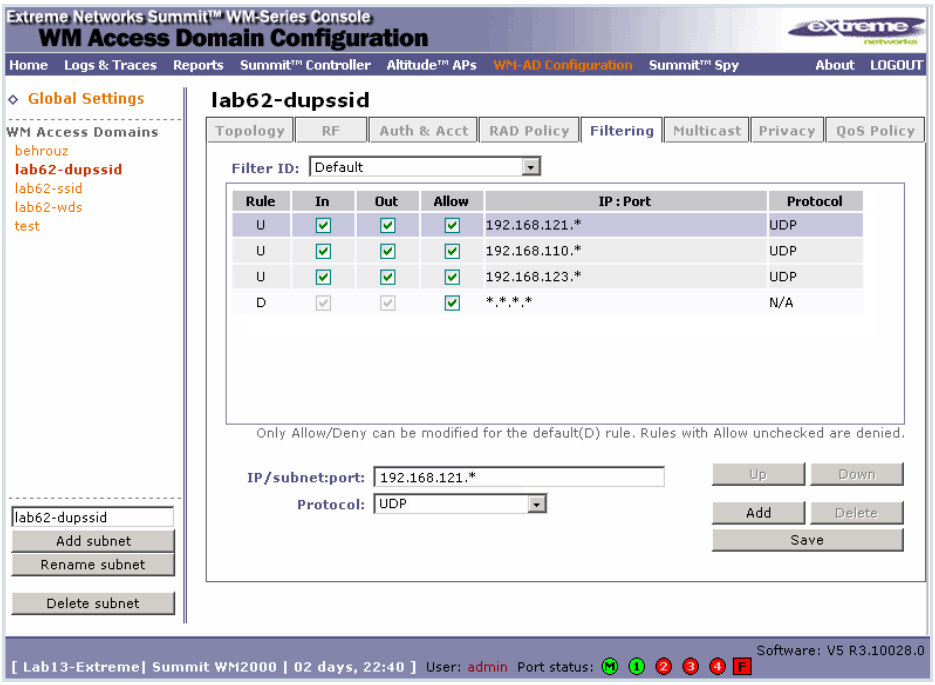
NOTE

*You must ensure that all the filtering rules, including the ones for SVP/Gateway and other network elements, are moved up, before the filtering rule for the **Default** filter.*

9 Select the **Allow** option of the **Default** filter.

10 Click **Save**.

The following screen-shot depicts how the configuration will appear in context of the network topology illustrated in Figure 34.


Extreme Networks Summit™ WM-Series Console
WM Access Domain Configuration
Home Logs & Traces Reports Summit™ Controller Altitude™ APs WM-AD Configuration Summit™ Spy About LOGOUT
Global Settings
WM Access Domains
behrouz
lab62-dupssid
lab62-ssid
lab62-wds
test
lab62-dupssid
Add subnet
Rename subnet
Delete subnet
lab62-dupssid
Topology RF Auth & Acct RAD Policy Filtering Multicast Privacy QoS Policy
Filter ID: Default
Rule In Out Allow IP : Port Protocol
U 192.168.121.* UDP
U 192.168.110.* UDP
U 192.168.123.* UDP
D *.*.*.* N/A
Only Allow/Deny can be modified for the default(D) rule. Rules with Allow unchecked are denied.
IP/subnet:port: 192.168.121.*
Protocol: UDP
Up Down Add Delete Save
Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 02 days, 22:40] User: admin Port status:

NOTE

You must complete the remaining configuration as explained in the subsequent sections, and then check if the deployment is working properly. If the deployment is working properly, you should deselect ***Allow*** *option of the* ***Default*** *filter in order to secure the network*
The secure setup in context of the network topology illustrated in Figure 34 will be as follows:
- Allow 192.168.121. UDP*
- Allow 192.168.110. UDP*
- Allow 192.168.123. UDP*
*- Disallow *.*.*.* N/A T*

Setting up Multicast configuration

NOTE

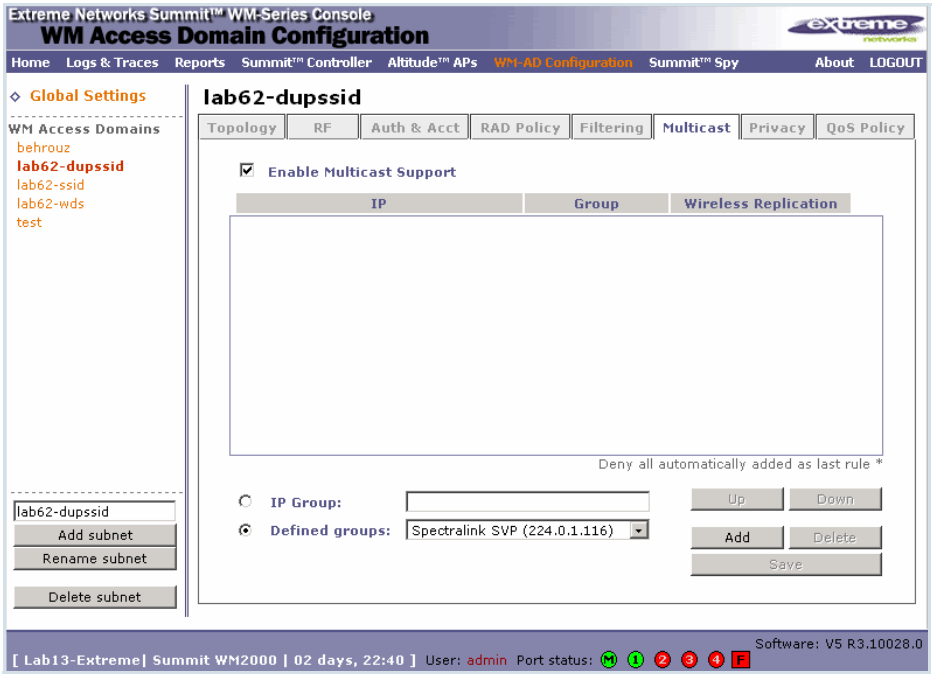
Before you set up multicast configuration, you must specify the physical port for routing multicast traffic on the ***Wireless Controller*** *configuration screen (****Wireless Controller Configuration>IP addresses****).*

To set up multicast configuration:

1. From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.
2. On the **WM Access Domain Configuration** screen, click the **Multicast** tab.
3. Select **Enable Multicast Support**.
4. From the **Defined groups** drop-down list, select **Spectralink SVP (224.0.1.116)** and then click **Add**.

5 Select **Wireless Replication** checkbox.

6 Click **Save** button.



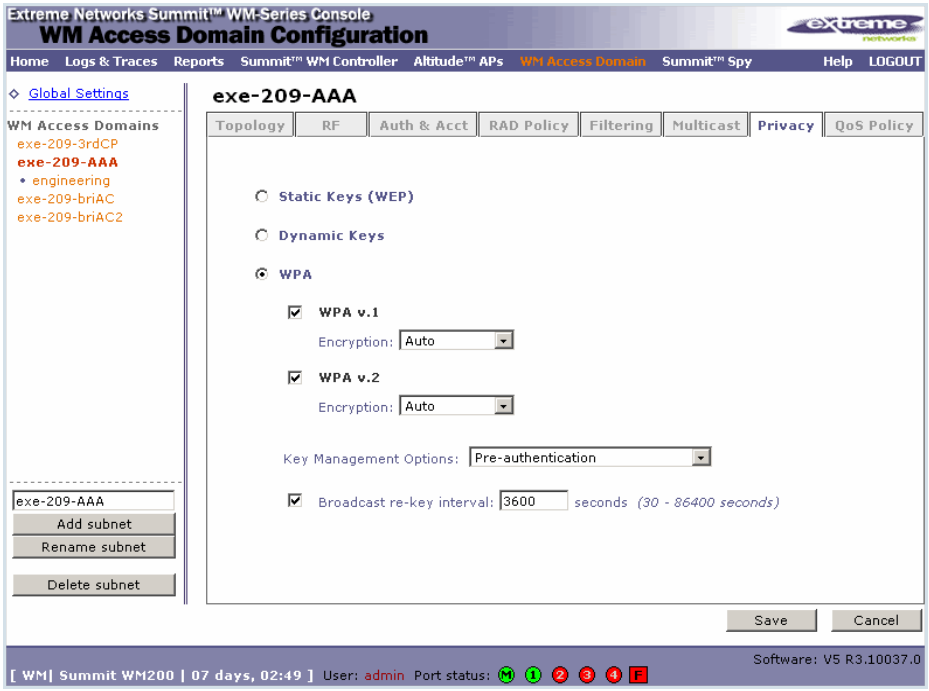
Setting up Security

To set up the security:

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 On the **WM Access Domain Configuration** screen, click the **Privacy** tab.

3 Select the **WPA-PSK** radio button.



4 Select the **WPA v.2** radio button.

5 Under **WPA v.2** section, select **AES** only from the **Encryption** drop-down menu.

NOTE

The SpectraLink telephones must also be for WPA v.2 security.

6 Enter the appropriate pass phrase in the **Pre-shared** key field.

7 Click **Save**.

Setting up Quality of Service (QoS)

To set up Quality of Service (QoS):

1 From the main menu, click **WM Access Domain Configuration**. The **WM Access Domain Configuration** screen is displayed.

2 On the **WM Access Domain Configuration** screen, click the **QoS Policy** tab.

3 Under the **Wireless QoS** section, select the following:

- Legacy
- Turbo Voice

NOTE

*If you are using Altitude APs and Outdoor APs, you must ensure that **Turbo Voice QoS** is selected to achieve best voice quality with the SpectraLink telephones. **Turbo Voice QoS** does not have any effect on Altitude 802.11n APs as these APs provide best voice quality regardless of whether **Turbo Voice QoS** is selected or not.*

NOTE

*To achieve "higher call capacity", you must ensure that **WMM** QoS is deselected.*

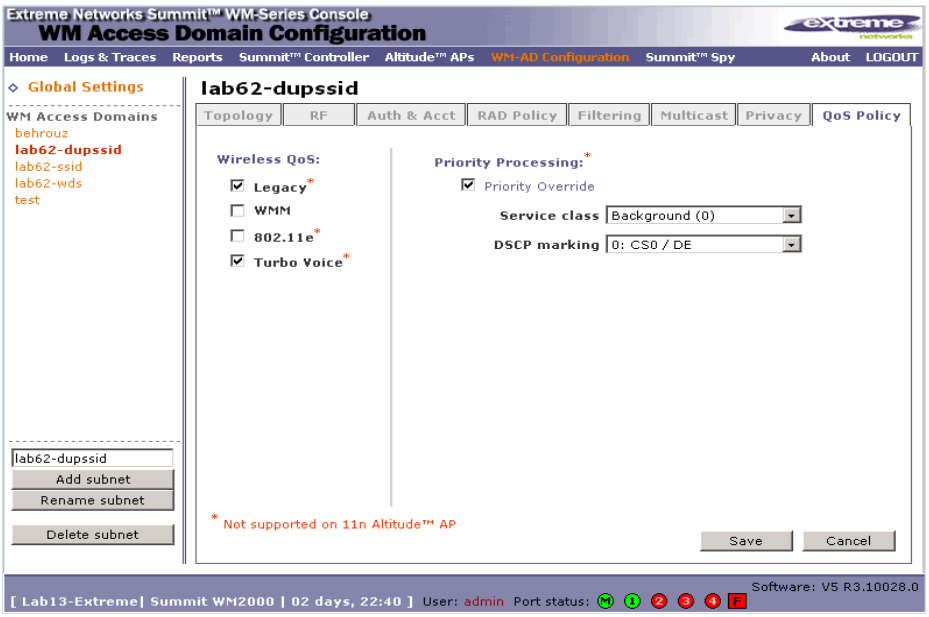
NOTE

*The Altitude 802.11n APs support only the **WMM** QoS. If you are using 802.11n APs, and you want to achieve "higher call capacity", you must ensure that **WMM** QoS is deselected. The **Turbo Voice** QoS does do not have any effect on the 802.11n APs regardless of whether it is selected or not.*

4 Under the **Priority Processing** section, select **Priority Override**.

5 Retain the default value in **Service Class** drop-down menu.

6 Retain the default value in **DSCP marking** drop-down menu.



7 Click **Save**.

Setting up Radio Properties

To set up the radio for Voice Wireless LAN in Altitude AP (Models 350-2i/350-2d):

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the list of Altitude APs, select the Altitude AP that is being used for the Voice WLAN.

3 On the **Altitude AP Configuration** screen, click **802.11b/g** or **802.11a/g**, depending upon the radio that is being used for Voice WLAN.

4 Under **Base Settings**, set the **DTIM Period** to **3**:

5 Under **Basic Radio Settings**, set the following parameters:

- **Tx Diversity**: Set the **Tx Diversity** to either **Left** or **Right**.
- **Total # of retries for Voice VO**: Set the **Total # of retries for Voice VO** to **adaptive (multi-rate)**.

NOTE

*It is recommended that the **Tx Diversity** should be set to **Left**.*

6 Retain the default values for all other parameters.

7 Click **Save**.

To set up the radio for Voice Wireless LAN in Altitude 802.11n APs:

1 From the main menu, click **Altitude AP Configuration**. The **Altitude AP Configuration** screen is displayed.

2 From the list of Altitude APs, select the Altitude 802.11n AP that is being used for the Voice WLAN.

3 On the **Altitude AP Configuration** screen, click **802.11b/g/n** or **802.11a/g/n**, depending upon the radio that is being used for Voice WLAN.

4 Under **Base Settings**, set the **DTIM Period** to **3**.

5 Retain the default values for all other parameters.

6 Click **Save**.

Index

A

about this guide, 9
accounting
  setup on a WM-AD, 179
ACS - Automatic Channel Selection, 89
adding
  Altitude AP manually, 84
allow or deny in a filtering rule, 147
Altitude AP
  802.1X, 116
    credentials, 121
    EAP-TLS, 117, 119
    multi-edit, 122
    PEAP, 117
  adding manually, 84
  assigning to a WM-AD, 165
  client disassociate, 297
  default configuration, 30, 72, 125, 134, 135
    copy to defaults, 134
  DRM, 88
  LED sequence in discovery, 73
  maintenance and reboot, 137
  radios, 88
  static configuration, 114
  view statistics, 277
Analysis engine
  functions, 267
ATPC - Auto Tx Power Control, 90
authentication
  MAC-based, 177
  no RADIUS server, 143
  none on a WM-AD, 202
  on a WM-AD for AAA, 174
  on a WM-AD for Captive Portal, 167
  overview of types, 166
  protocols supported, 145, 169
Authentication, Authorization, Accounting (AAA)
  set up 802.1X authentication, 174
  set up privacy on a WM-AD, 196

B

back panel, Summit WM Controller WM200/2000, 333
branch office, static configuration of Altitude AP, 114

C

call data records (CDRs), 179
Captive Portal
  authentication on a WM-AD, 167
  configuring internal, external Captive Portal, 172
  defined, 145
  non-authenticated filtering rules, 183
  privacy mechanisms, 193
  set up a WM-AD topology, 157
  view sample page, 173
codes, LED states and seven segment display, 331
configuring
  Captive Portal, internal, external, 172
  software - overview steps, 25
  static routes, 43
controller
  availability overview, 24

D

default filter, 189
default gateway on a WM-AD, 160
disassociate a wireless client, 297
discovery
  Altitude AP LED sequence, 73
  steps, 71
displays
  Altitude AP wired and wireless statistics, 277
  client location by foreign WM, 283
  client location by home, 283
  list of displays, 273
  WM tunnel traffic, 283
documentation feedback, 11
Domain Name Server (DNS)
  in discovery, 71
DRM - Dynamic Radio Management, 89
DSCP classifications, 207
Dynamic Host Configuration Protocol (DHCP)
  Option 78 in discovery, 71
  relay on a WM-AD, 162
  required as part of solution, 17

E

exception filters

on a WM-AD, 182
port-based, 49
exclusions, IP address range on a WM-AD, 161

F

failover of a controller
availability overview, 24
failover of a RADIUS server, 170
filtering
default filter, 189
exception filter on a WM-AD, 182
filtering rules, overview of set up, 181
for an AAA group, 191
for Captive Portal authentication, 173
non-authenticated filter for Captive Portal, 183
non-authenticated filtering rules, examples, 186
on a WM-AD for third-party APs, 261
overview of packet filtering, 23
overview, four types, 146
port-based, 48
rules for filter ID values, 187
set filter ID values (RADIUS policy), 180
formatting conventions, 10
forwarding table report, 44

G

gateway, default, on a WM-AD, 160
global settings
for a WM-AD, 149
RADIUS servers for authentication, 169, 175, 177, 179
guide, about this, 9

I

IP address range on a WM-AD, 161

K

key management options
none, 199
opportunistic keying, 200
opportunistic keying & pre-auth, 200
pre-authentication, 200

L

LED sequence
in discovery, 73
LED states and seven segment display (SSD) codes, 331
login user name and password, 32
Login-LAT-Group, 187

M

MAC-based authentication, 177
management port
management traffic on data port, 39
port-based filtering, 48
management traffic
enabling on a WM-AD, 159
mobility
overview, 24
multicast
for a WM-AD, 191

N

network assignment
by AAA, 196
by SSID for Captive Portal, 157
options for a WM-AD, 143
VLAN, 18
network security, overview, 21
next hop route for a WM-AD, 160
non-authenticated filter for Captive Portal, 173, 183
ntrol, 90

O

OSPF
configuring, 45
linkstate report, 47
neighbor report, 47
on a WM-AD, 160
overview, 23

P

port
port exception filters, 49
priority override, 204
privacy
dynamic WEP on a WM-AD for AAA, 198
encryption methods supported, 22
on a WM-AD for AAA
AAA, 196
overview on a WM-AD, 148
setup on a WM-AD for Captive Portal, 193
static WEP for an AAA WM-AD, 197
WPA v1 and WPA v2 on a WM-AD for AAA, 198
protocols
for authentication by Captive Portal, 169

Q

QoS (Quality of Service), 25, 143, 150, 151, 203, 204, 317, 320
admission control thresholds, 150
advanced, 207
modes, 204
policy, 206

R

radio
channels, 92, 106, 114
radio settings
view and modify, 88
RADIUS server
deployment with no server, 143
filter ID values, 187
for authentication, 169, 175, 177, 179
for MAC-based authentication, 177
priority for redundancy, 170
RADIUS accounting, 179
RADIUS policy for a WM-AD, 180
required as part of solution, 17
VSAs in RADIUS message, 166
reboot Altitude AP, 137
reports
AP inventory, 285
forwarding table, 44, 285
list of displays, 273
OSPF linkstate, 47, 285
OSPF neighbor, 47, 285
rogue detection, Summit WM series Spy feature, 268
routing
configuring OSPF on data port, 45
configuring static routes, 43
next hop route on a WM-AD, 160
overview, 23
routing table
viewing, 44

S

scan results, Summit WM series Spy feature, 268
service class, 203
Service Location Protocol (SLP)
in discovery, 71
required as part of solution, 17
traffic allowed on data port, 39
software
maintenance of Altitude AP software, 137
SSID network assignment for Captive Portal, 157
static configuration of Altitude AP, 114
static routes
configuring, 43
viewing forwarding table report, 44
Summit WM Controller WM200/2000 back panel, 333

T

third-party APs
defining a WM-AD for, 159
topology of a WM-AD
Captive Portal, 157
Type of Service (ToS/DSCP)
on a WM-AD, 203
Quality of Service, 25

U

user name and password for login, 32

V

vendor specific attributes (VSA)
in RADIUS message, 166
RADIUS server
vendor specific attributes, 170, 176
VLAN, 321
configuration, 115, 156, 160, 204, 209, 211
IDs, 211
Voice-over-IP (VoIP)
define multicast groups on a WM-AD, 191
set up a WM-AD for, 203

W

WDS
deployment, 220
examples of deployment, 214
key features, 217
overview, 212
simple configuration, 212
wireless bridge configuration, 213
wireless repeater configuration, 213
WM-AD, 214
WDS - Wireless Distribution System, 212
Wi-Fi Multimedia (WMM)
on a WM-AD, 203
Quality of Service, 25
Wi-Fi Protected Access (WPA)
overview on a WM-AD, 148
PSK mode for Captive Portal, 195
WPA v1 and v2 on a WM-AD for AAA, 198
Wired Equivalent Privacy (WEP)
on a WM-AD for AAA, 197
overview on a WM-AD, 148

static for Captive Portal, 194
WM Access Domain Services, 23
WM Access Domain Services (WM-AD)
authentication by AAA (802.1X), 174
authentication by Captive Portal, 167
define filtering rules, 181
defined, 141
for third-party APs, 260
global settings, 149
multicast, 191
network assignment overview, 143
privacy for AAA, 196
privacy overview, 193
set up for VoIP, 203
topology for Captive Portal, 157